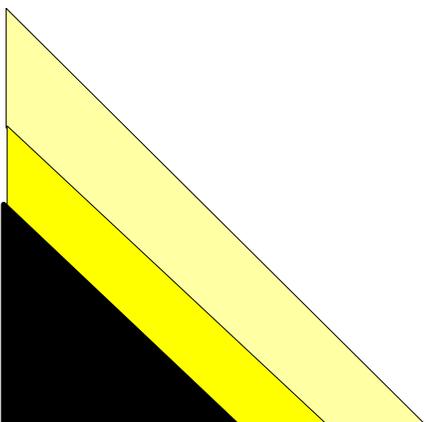
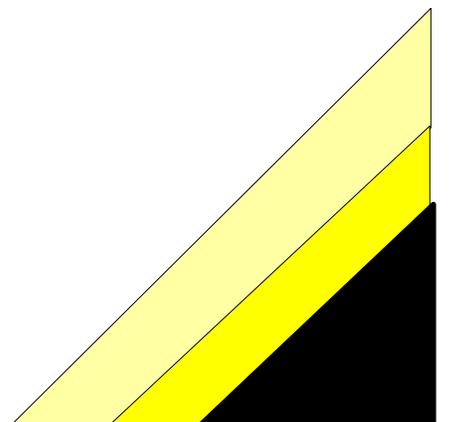




# **US EMPLOYEE HANDBOOK**



*Revised February 2017*



## **TABLE OF CONTENTS**

INTRODUCTION TO THE HANDBOOK.....	4	MOBILE DEVICES .....	24
Equal Employment Opportunity and Prohibited Discrimination .....	4	Mobile Device Expense Reimbursement.....	24
Conflict of Interest and Outside Employment Statement .....	6	Mobile Device Hands-Free Policy.....	25
Confidential Nature of Work .....	7	Mobile Device Physical Asset Security.....	25
EMPLOYMENT.....	7	Travel Security Precautions for mobile devices .....	25
Employment Introductory Period .....	7	Mobile Device Acceptable Use .....	25
Employment at Will .....	8	Telenav Issued Devices.....	25
Employee Categories .....	8	Employee-owned (BYOD) Devices.....	25
Transfers & Promotions .....	8	Technical Requirements .....	25
COMPENSATION .....	8	Mobile Device Configuration.....	25
Payment of Wages .....	8	Mobile Password Requirements .....	26
Overtime Pay .....	9	Mobile Device Updates .....	26
Time Records .....	9	Remote Wipe Capability .....	26
Meal Periods.....	9	Use of Company Equipment.....	26
Personnel Records .....	10	Photography and Recording Restrictions .....	26
TIME OFF.....	10	Audio Recording Policy.....	27
Leaves of Absence .....	10	PHYSICAL SECURITY .....	27
Family Care & medical Leave (California Family Rights Act leave).....	10	Photo ID/Access Badges .....	27
Pregnancy Disability Leave .....	12	A) Employees.....	27
Other Disability Leaves.....	13	B) Contractors/Consultants, Interns and Temporary Employees.....	27
Military Leave.....	14	C) Visitors .....	27
Jury & Witness Duty .....	16	Authorized Access Only.....	28
Leave for Educational/Daycare Purposes .....	17	Protect Sensitive Information .....	28
Voting Time Off.....	17	Storing Data on Laptops .....	28
Bereavement Leave.....	17	Accountability.....	28
Sick Leave .....	17	Reporting Incidents .....	28
Holidays .....	18	Lost or Stolen Device.....	28
BENEFITS OVERVIEW.....	19	IT SYSTEMS POLICY.....	28
ON THE JOB .....	19	No expectation of privacy .....	30
Seminars, Professional, Certifications and Related Membership Dues.....	19	Remote Access.....	30
Attendance, Punctuality and Dependability .....	19	Third-Party Remote Access.....	30
Work from Home.....	19	VPN Access .....	31
Drugs & Drug Abuse.....	20	Multiple Networks Connections .....	31
Alcohol & Alcohol Abuse.....	20	Wireless Acceptable Use .....	31
Appearance, Conduct & Language .....	20	Internet Use Policy.....	31
Anti-Nepotism policy.....	20	Internet Acceptable Use.....	31
Romantic or Sexual Relationships.....	21	Disclaimer of liability for use of Internet .....	31
Injury And Illness Prevention Program .....	21	Duty not to waste computer resources .....	31
Violence in the Workplace .....	21	Email and Electronic Communications Systems Acceptable Use.....	32
Accidents & Emergencies.....	21	E-Mail Retention Policy.....	32
Smoking Policy .....	22	Acceptable Use of Software .....	32
Open Door Policy.....	22	Removable Media Acceptable Use.....	32
Internal Complaint Procedures .....	22	Social Media .....	32
Fraud / Dishonesty / Ethics.....	22	Professionalism.....	33
Solicitations, Distributions and Use of Bulletin Boards.....	23	Confidential Information .....	33
Internal Investigation & Searches .....	23	Conflicts of Interest .....	33
Reference Checks .....	23	Truthfulness .....	33
Emergency Closing Policy .....	23	Personal and Proprietary Information.....	33
		Legality.....	33

---

Positivity.....	33	Password Storage.....	35
Solicitation and Marketing.....	33	Encrypted Transmission .....	35
Public Relations .....	33	Credential Communications.....	35
Telenav Trademarks.....	33	Administrator Password Requirements .....	35
Social Media Privacy .....	33	Prohibited Password Security Activities.....	36
Policies Apply .....	33	Report Incidents.....	36
Enforcement .....	33	LEAVING TELENAV .....	36
Consent to Monitoring.....	34	Employer Information and Property .....	36
Unacceptable Use .....	34	Resignation .....	36
Blocking of Inappropriate Content .....	34	Dismissals.....	36
Prohibited Activities .....	34	EMPLOYEE CODE OF CONDUCT .....	37
Illegal copying .....	34	Discipline other than Immediate Discharge ...	37
Virus detection .....	34	Post Resignation/Discharge Procedures .....	37
PASSWORD REQUIREMENTS .....	35	ACKNOWLEDGMENT OF RECEIPT OF	
Account Lockout .....	35	EMPLOYEE HANDBOOK .....	39
Password Protection Requirements .....	35		

---

## **INTRODUCTION TO THE HANDBOOK**

Welcome to Telenav. This handbook is designed to help US employees get acquainted with some of Telenav's philosophies and beliefs, and in general terms describes some of our employment guidelines. This handbook is meant to highlight some of our Company policies, and general benefits information for US employees. We hope that it will serve as a useful reference document for employees throughout their employment at Telenav. Employees should understand, however, that this handbook is not intended to be a contract (express or implied), nor is it intended to otherwise create any legally enforceable obligations on the part of Telenav or its employees. Except as otherwise provided, this handbook supersedes and replaces all previous Human Resource policies, practices, and guidelines.

Because Telenav is a growing and changing organization, it reserves full discretion to add to, modify, or delete provisions of this handbook, or the policies and procedures on which they may be based, at any time without notice. The only exception to this is the Company's policy of at-will employment, which can only be modified in writing, signed by the CEO of the Company. Telenav also reserves the right to interpret any of the provisions set forth in this handbook in any manner it deems appropriate. For this reason, employees should check with their immediate Supervisor or the Human Resource Department to obtain current information regarding the status of any policy, procedure, guideline, or practice. Similarly, to obtain information regarding specific employment policies or procedures, whether they are contained in this handbook, employees should contact the Human Resource Department.

No individual other than the Company CEO has the authority to enter into any employment agreement, for any specified term or that otherwise modifies the at-will relationship between the Company and any of its employees. Any such agreements *must* be in writing, signed both by the Company CEO and the affected employee. This handbook is the property of Telenav, and it is intended for personal use and reference by employees of the Company. Circulation of this handbook outside of Telenav requires the prior written approval of the Human Resource Manager.

Employees should read this handbook on Telenav's policy library portal and click to acknowledgement receipt of the Employee Handbook within their first week of employment with the company. This will provide the Company with a record that each employee has received this handbook.

## **EQUAL EMPLOYMENT OPPORTUNITY AND PROHIBITED DISCRIMINATION**

Telenav is an equal opportunity employer and is committed to preventing discrimination, harassment and retaliation in the workplace. In accordance with applicable law, we prohibit discrimination against employees, applicants for employment, individuals providing services in the workplace pursuant to a contract, unpaid interns and volunteers based on their actual or perceived: race, religious creed, color, national origin, ancestry, physical or mental

disability, medical condition, genetic information, marital status, sex (including pregnancy, childbirth, lactation and their related medical conditions), gender (including gender identity and expression), age, sexual orientation, military and veteran status and any other consideration protected by federal, state or local law (sometimes referred to, collectively, as "protected characteristics").

Our commitment to equal employment opportunity applies to all persons involved in our operations and prohibits unlawful discrimination and harassment by any employee (including supervisors, managers and co-workers), agent, client, customer, or vendor. Federal, California and local laws forbid these individuals from engaging in conduct prohibited by the applicable laws.

### **PROHIBITED HARASSMENT**

Telenav is committed to providing a work environment that is free of illicit harassment based on any protected characteristics. As a result, the Company maintains a strict policy prohibiting sexual harassment and harassment against employees, applicants for employment, individuals providing services in the workplace pursuant to a contract, unpaid interns or volunteers based on any legally-recognized basis, including, but not limited to, their actual or perceived race, religious creed, color, national origin, ancestry, physical or mental disability, medical condition, genetic information, marital status, sex (including pregnancy, childbirth, lactation and their related medical conditions), gender (including gender identity and expression), age, sexual orientation, military and veteran status, or any other consideration protected by federal, state or local law. All such harassment is prohibited.

This policy applies to all persons involved in our operations, including coworkers, supervisors, managers, temporary or seasonal workers, agents, clients, vendors, customers, or any other third party interacting with the Company ("third parties") and prohibits proscribed harassing conduct by any employee or third party of Telenav, including nonsupervisory employees, supervisors and managers. Regardless of where such harassment occurs and is directed toward an employee or a third party interacting with the Company, the procedures in this policy should be followed.

Telenav will provide a reasonable accommodation for any known physical or mental disability of a qualified individual or for employees' religious beliefs and observances, provided the requested accommodation does not create an undue hardship for the Company and does not pose a direct threat to the health or safety of others in the workplace or to the individual. The Company will not retaliate or discriminate against a person for requesting an accommodation for his or her disability, regardless of whether the accommodation was granted.

### **DEFINITIONS OF HARASSMENT**

Sexual harassment includes unwanted sexual advances, requests for sexual favors or visual, verbal or physical conduct of a sexual nature when:

- Submission to such conduct is made a term or condition of employment; or

- Submission to, or rejection of, such conduct is used as a basis for employment decisions affecting the individual; or
- Such conduct has the purpose or effect of unreasonably interfering with an employee's work performance or creating an intimidating, hostile or offensive working environment.

Sexual harassment also includes various forms of offensive behavior based on sex and includes gender-based harassment of a person of the same sex as the harasser. The following is a partial list:

- Unwanted sexual advances.
- Offering an employment benefit (such as a raise, promotion or career advancement) in exchange for sexual favors, or threatening an employment detriment (such as termination or demotion) for an employee's failure to engage in sexual activity.
- Visual conduct: leering, making sexual gestures and displaying or posting sexually suggestive objects, pictures, cartoons, posters, websites, emails or text messages.
- Verbal conduct: making or using derogatory comments, epithets, slurs, sexually explicit jokes, or comments about an employee's body or dress.
- Verbal sexual advances, propositions, requests or comments.
- Sending or posting sexually related messages, videos or messages via text, instant messaging or social media.
- Verbal abuse of a sexual nature, graphic verbal comments about an individual's body, sexually degrading words used to describe an individual and suggestive or obscene letters, notes or invitations.
- Physical conduct, such as touching, groping, assault or blocking movement.
- Physical or verbal abuse concerning an individual's gender, gender identity or gender expression.
- Verbal abuse concerning a person's characteristics such as pitch of voice, facial hair or the size or shape of a person's body, including remarks that a male is too feminine or a woman is too masculine.

An employee may violate this policy against sexual harassment even if the alleged harassing conduct was not motivated by sexual desire. An employee who engages in harassment may be personally liable for harassment even if the Company had no knowledge of such conduct.

***Other examples of prohibited harassment or discrimination***

In addition to the above listed conduct, the Company strictly prohibits harassment or discrimination concerning any other protected characteristic. Such prohibited harassment includes:

- Racial or ethnic slurs, epithets and any other offensive remarks.
- Jokes, whether written, verbal or electronic.
- Threats, intimidation and other menacing behavior.
- Inappropriate verbal, graphic or physical conduct.

- Sending or posting harassing messages, videos or messages via text, instant messaging or social media.
- Other harassing or discriminatory conduct based on one or more of the protected categories identified in this policy.

Employees who have any questions about what constitutes harassing or discriminatory conduct should contact their supervisor or Human Resources.

**INDIVIDUALS AND CONDUCT COVERED**

This Company prohibits unlawful discrimination and harassment in the workplace and applies to applicants and employees of the Company, including supervisors and managers. The Company prohibits managers, supervisors and employees from discriminating against or harassing co-workers as well as customers, vendors, suppliers, independent contractors and others doing business with the company. In addition, the Company prohibits customers, vendors, suppliers, independent contractors and others doing business with the Company from discriminating against or harassing the Company's employees.

**REPORTING HARASSMENT OR DISCRIMINATION**

If an employee feels that he or she is being harassed or discriminated against in violation of this policy by another employee, supervisor, manager or third party doing business with the Company, the employee should immediately contact their supervisor or Human Resources. Employees are not required to make a complaint directly to their immediate supervisor. In addition, if an employee observes harassment or discrimination by another employee, supervisor, manager or nonemployee, the employee should immediately report the incident to the individuals identified above. Appropriate action will also be taken in response to violation of this policy by any nonemployee.

Supervisors must report complaints of misconduct under this policy to Human Resources immediately so the company can investigate and try to resolve the claim internally.

Complaints of unlawful harassment or discrimination that are reported to management or to the persons identified above will be investigated as promptly as possible, and corrective action will be taken where warranted. Complaints will be investigated by impartial and qualified internal personnel unless external involvement is warranted. Complaints of unlawful harassment or discrimination that are reported to management or to the persons identified above will be treated with as much confidentiality as possible, consistent with the need to conduct an adequate investigation. The Company expects all employees to fully cooperate with any investigation conducted by the Company into a complaint of proscribed harassment, discrimination or retaliation, or regarding the alleged violation of any other Company policies. The process will be documented and tracked for reasonable progress, and investigations will be completely timely.

The California Department of Fair Employment and Housing (DFEH), the federal Equal Employment Opportunity Commission (EEOC) and the California Department of Fair Employment and Housing

(DFEH) or other federal, state and local agencies, may also investigate and process complaints of harassment or discrimination. Violators are subject to penalties and remedial measures that may include sanctions, fines, injunctions, reinstatement, back pay and damages. The toll-free number from the DFEH is (800) 884-1684. Information may be located by visiting the agency website at [www.eeoc.gov](http://www.eeoc.gov) or [www.dfeh.ca.gov](http://www.dfeh.ca.gov).

Employees' notification to the Company is essential to enforcing this policy. Employees may be assured that they will not be penalized in any way for reporting a harassment or discrimination problem. It is unlawful for an employer to retaliate against employees who oppose the practices prohibited by the California Fair Employment and Housing Act (FEHA) or other federal, state or local regulations, or who file complaints or otherwise participate in an investigation, proceeding or hearing conducted by the California Department of Fair Employment and Housing (DFEH), the Fair Employment and Housing Commission (FEHC), the EEOC or other federal, state and local agencies. Similarly, the company prohibits employees from hindering its internal investigations or its internal complaint procedure.

#### **VIOLATIONS OF THIS POLICY WILL RESULT IN DISCIPLINE**

Violation of this policy will subject an employee to disciplinary action, up to and including immediate termination. In addition, under California law, employees may be held personally liable for harassing conduct that violates the FEHA, as well as various other federal, state and local agencies.

#### **RETALIATION IS PROHIBITED**

Telenav prohibits retaliation against those who report, oppose or participate in an investigation of alleged violations of this policy. Participating in an investigation of alleged wrongdoing in the workplace includes:

- Filing a complaint with a federal or state enforcement or administrative agency.
- Participating in or cooperating with a federal or state enforcement agency that is investigating of the company regarding alleged unlawful activity.
- Testifying as a party, witness or accused regarding alleged unlawful activity.
- Associating with another employee who is engaged in any of these activities.
- Making or filing an internal complaint with the company regarding alleged unlawful activity.
- Providing informal notice to the company regarding alleged unlawful activity.

Prohibited retaliation includes, but is not limited to, termination, demotion, suspension, failure to hire or consider for hire, failure to give equal consideration in making employment decisions, failure to make employment recommendations impartially, adversely affecting working conditions or otherwise denying any employment benefit.

The Company strictly prohibits any adverse action or retaliation against an employee for participating in an investigation of alleged violation of this policy. If an employee feels that he or she is being retaliated

against, the employee should immediately contact their supervisor, Human Resources, or the General Counsel. In addition, if an employee observes retaliation by another employee, supervisor, manager or nonemployee, he or she should immediately report the incident to the individuals identified above.

Any employee determined to be responsible for violating this policy will be subject to appropriate disciplinary action, up to and including termination. Moreover, any employee, supervisor or manager who condones or ignores potential violations of this policy will be subject to appropriate disciplinary action, up to and including termination.

#### **CONFLICT OF INTEREST AND OUTSIDE EMPLOYMENT STATEMENT**

Telenav expects our employees to conduct business according to the highest ethical standards of conduct. Employees are expected to devote their best efforts to the interests of the Company. Business dealings that appear to create a conflict between the interests of the Company and an employee are unacceptable. The Company recognizes the right of employees to engage in activities outside of their employment, which are lawful, of a private nature and unrelated to our business. However, the employee must disclose any possible conflicts so that the Company may assess and prevent potential conflicts of interest from arising. A potential or actual conflict of interest occurs whenever an employee is in a position to influence a decision that may result in a personal gain for the employee or an immediate family member (i.e., spouse or significant other, children, parents, siblings) as a result of the Company's business dealings.

Although it is not possible to specify every action that might create a conflict of interest, this policy sets forth those that most frequently present problems. If an employee has any question whether an action or proposed course of conduct would create a conflict of interest, he or she should immediately contact their Direct Supervisor or the Human Resources Department to obtain advice on the issue. The purpose of this policy is to protect employees from any conflict of interest that might arise.

A violation of this policy will result in immediate and appropriate discipline, up to and including immediate discharge.

#### **OUTSIDE EMPLOYMENT**

Employees are required to obtain written approval from their supervisor and the Human Resources Department before participating in outside work activities. Approval will be granted unless the activity conflicts with the Company's interest. In general, outside work activities are not allowed when they:

- prevent the employee from fully performing work for which he or she is employed at the Company, including overtime assignments;
- involve organizations that are doing or seek to do business with the Company, including actual or potential vendors or customers; or

- violate provisions of law or the Company's policies or rules.

From time to time, Company employees may be required to work beyond their normally scheduled hours. Employees must perform this work when requested. In cases of conflict with any outside activity, the employee's obligations to the Company must be given priority. Employees are hired and continue in Telenav's employ with the understanding that Telenav is their primary employer and that other employment or commercial involvement that conflicts with the business interests of Telenav is strictly prohibited.

### **FINANCIAL INTEREST IN OTHER BUSINESS**

An employee and his or her immediate family may not own or hold any significant interest in a supplier, customer, or competitor of the Telenav, except where such ownership or interest consists of securities in a publicly owned company and such securities are regularly traded on the open market and the holdings constitute less than 5% of such entity.

### **ACCEPTANCE OF GIFTS**

No employee may solicit or accept gifts of significant value, lavish entertainment or other benefits from potential and actual customers, suppliers, or competitors of Telenav. Special care must be taken to avoid even the impression of a conflict of interest.

An employee may entertain potential or actual customers if such entertainment is consistent with accepted business practices, does not violate any law or generally accepted ethical standards and the public disclosure of facts will not embarrass the Company. Any questions regarding this policy should be addressed to the Human Resources Department.

### **WORK PRODUCT OWNERSHIP**

All Telenav employees must sign a Proprietary Information Agreement when they accept our offer of employment and be aware that Telenav retains legal ownership of the product of their work to the extent permitted by applicable law. No work product created while employed by Telenav can be claimed, construed, or presented as property of the individual, even after employment by Telenav has been terminated or the relevant project completed. This includes written and electronic documents, audio and video recordings, system code, and any concepts, ideas, or other intellectual property developed for Telenav, regardless of whether the intellectual property is used by Telenav. Although it is acceptable for an employee to display and/or discuss a portion or the whole of certain work product as an example in certain situations (e.g., on a resume, in a freelancer's meeting with a prospective client), one must bear in mind that information classified as confidential must remain so even after the end of employment, and that supplying certain other entities with certain types of information may constitute a conflict of interest. In any event, it must always be made clear that work product is the sole and exclusive property of Telenav. Freelancers and temporary employees must be particularly careful in the course of any work they discuss doing, or actually do, for a competitor of Telenav.

### **REPORTING POTENTIAL CONFLICTS**

An employee must promptly disclose actual or potential conflicts of interest, in writing, to his or her supervisor. Approval will not be given unless the relationship will not interfere with the employee's duties or will not damage the Company's relationship.

### **CONFIDENTIAL NATURE OF WORK**

All Telenav records and information relating to Telenav or its customers are confidential and employees must, therefore, treat all matters accordingly. No Telenav or Telenav-related information, including without limitation, documents, notes, files, records, oral information, computer files or similar materials (except in the ordinary course of performing duties on behalf of Telenav) may be removed from Telenav's premises without permission from Telenav; provided however, Telenav-issued laptops may be used outside of Telenav's premises to perform duties on behalf of Telenav. Additionally, the contents of Telenav's records or information otherwise obtained in regards to business may not be disclosed to anyone, except where required for a business purpose. Employees must not disclose any confidential information, purposefully or inadvertently through casual conversation, to any unauthorized person inside or outside the Company. Employees who are unsure about the confidential nature of specific information must ask their supervisor for clarification. Employees will be subject to appropriate disciplinary action, up to and including discharge, for knowingly or unknowingly revealing information of a confidential nature known from other employees, customers, or others, as agreed upon in the Non-Disclosure Statement signed at the time of employment acceptance.

## **EMPLOYMENT**

### **EMPLOYMENT INTRODUCTORY PERIOD**

Telenav attempts to hire and/or promote the most-qualified employees for each position. To ensure this, Telenav provides for an introductory period of employment for the employee to assess Telenav and the job content of the position accepted, and for Telenav to evaluate the new employee and his or her job performance. All new employees must complete, to Telenav's satisfaction, a 90-day introductory period beginning with the date of initial employment. (This 90-day period is defined by actual days worked.) During this time, the new employee will be provided with training and guidance from his/her Supervisor and the Company. This introductory period does not change the employee's status as an at-will employee and is not a guarantee of employment for any duration. An employee may be discharged at any time during this period if his/her Supervisor concludes that he/she is not progressing or performing satisfactorily or for any other reason with or without prior notice. Similarly, the employee may resign employment for any reason without prior notice during this period.

Upon successful completion of the introductory period, an employee will become a regular employee. Under appropriate circumstances, the Company may also extend the introductory period. Additionally, as is true at all times during an

employee's employment with the Company, employment is not for any specific time and may be terminated at will, with or without cause and without prior notice. Completion of the introductory period does not modify this at-will relationship and does not provide a guarantee of continued employment.

Introductory periods will also be used when an employee is promoted or transferred into a new role with new job functions within the Company. The 90-day introductory period will begin on the date that the employee's title changes.

## **EMPLOYMENT AT WILL**

Employment at Telenav may be terminated for any reason, with or without cause or notice, at any time by the employee or the Company. Nothing in this Employee Handbook or in any oral or written statement shall limit the right to terminate employment at will. No manager or employee of the Company shall have any authority to enter into an employment agreement--express or implied--with any employee providing for employment other than at-will.

This policy of at-will employment is the sole and entire agreement between you and the Company as to the duration of employment and the circumstances under which employment may be terminated.

Except for employment at will, terms and conditions of employment with the Company may be modified at the sole discretion of the Company with or without cause or notice at any time. No implied contract concerning any employment-related decision or term or condition of employment can be established by any other statement, conduct, policy, or practice. Examples of the types of terms and conditions of employment that are within the sole discretion of the Company include, but are not limited to, the following: promotion; demotion; transfers; hiring decisions; compensation; benefits; qualifications; discipline; layoff or recall; rules; hours and schedules; work assignments; job duties and responsibilities; production standards; subcontracting; reduction, cessation, or expansion of operations; sale, relocation, merger, or consolidation of operations; decisions concerning the use of equipment, methods, or facilities; or any other terms and conditions that the Company may determine to be necessary for the safe, efficient, and economic operation of its business.

## **EMPLOYEE CATEGORIES**

Based on the conditions of employment, employees of Telenav fall into the following categories:

- **Full-Time:** An employee who works a regular schedule of at least 30 hours for the Company each week.
- **Part-Time:** Part-time employees work a regular schedule of less than 30 hours for the Company each week. Part-time employees are not eligible for company paid benefits and company paid time off.
- **Temporary:** At times the Company may hire temporary employees to assist in projects and immediate needs. Temporary employees may be employed directly by the

Company or through a third-party employment agency. Temporary employees are not eligible for company paid benefits and company paid time off.

- **Exempt:** Exempt employees are classified as such if their job duties are exempt from the overtime provisions of the federal and state wage and hour laws. Exempt employees are not eligible for overtime pay. Their salaries are calculated on a weekly basis.
- **Non-Exempt:** Non-exempt employees receive overtime pay in accordance with our overtime policy and applicable federal and state wage and hour laws. Their salaries are calculated on an hourly basis.

## **TRANSFERS & PROMOTIONS**

Telenav encourages employees to assume higher-level positions or lateral transfers for which they qualify.

Generally, employees must be in their job for at least one (1) year before applying for a change in position. In addition, employees must have a good performance, attendance and punctuality record.

Each employee requesting a transfer will be considered for the new position along with all other applicants.

Each transfer is judged on an individual basis, depending on the needs of both departments involved.

Department Management will make all final decisions regarding transfers, in conjunction with the Human Resources Department.

Employees who wish to apply for a transfer should discuss it first with their direct supervisor/manager and the Human Resources Department so that it may be determined if their skills fit the requirements of the desired job. Employees should also feel free to discuss their career aspirations with their supervisor/manager or the Human Resources Department at any time.

## **COMPENSATION**

### **PAYMENT OF WAGES**

Payment of an employee's regular base wages is made semi-monthly for all hours worked up to the pay date. Paydays generally fall on the 15<sup>th</sup> and the last day of every month.

Payment for overtime hours worked, which is included with the non-exempt employee's base salary payment, is also paid semi-monthly with such payment covering hours worked in the current semi-monthly period. (For additional explanations see section on overtime policy and procedures.) In instances where employee receives a physical check, it is the Company's policy that paychecks will only be given to that employee. All other arrangements for mailing or pick-up must be made in advance and in writing with Payroll.

If the normal payday falls on a Company-recognized holiday, payment will be made one workday prior to the aforementioned schedule. Under no circumstances will the Company release any paychecks prior to the announced schedule.

Employees may be paid through direct deposit of funds to either a savings or checking account at their bank of choice (providing the bank has direct deposit capability). To activate direct deposit, a Direct Deposit Authorization form may be obtained from Human Resources or on the company intranet. The completed form must then be returned with a voided personal check to the Payroll Department. Due to banking requirements, it may take several weeks for activation of the Direct Deposit.

In the event of a lost paycheck, the Human Resources Department must be notified in writing as soon as possible.

The number of exemptions claimed on Form W-4, Employee's Withholding Allowance Certificate, affects the amount of Federal withholding. If an employee's marital status changes or the number of exemptions previously claimed increases or decreases, a new Form W-4 must be submitted to the Human Resources Department.

No salary advances will be made.

## OVERTIME PAY

Depending on Company work needs, employees will be required to work overtime when requested to do so. Prior approval of a supervisor, however, is required before any non-exempt employee works overtime. Employees working overtime without approval will be subject to disciplinary action. Your regular working schedule at Telenav are determined by your Direct Supervisor.

A. Overtime Definition and Rates of Pay: All nonexempt employees who work more than eight (8) hours in one workday or more than forty (40) hours in one work week will receive overtime pay computed as follows:

(1) Overtime at the rate of 1 1/2 times the employee's regular rate of pay for all hours worked in excess of forty (40) in any one work week.

(2) Overtime at the rate of 1 1/2 times the employee's regular rate of pay for the first four hours worked in excess of eight hours in any one workday and for the first eight hours on the seventh day of work in any one workweek.

(3) Overtime at the rate of double the employee's regular rate of pay for all hours worked in excess of twelve in one workday and for all hours worked in excess of eight on the seventh day of work in one work week.

Only those hours that are actually worked are counted to determine an employee's overtime pay. Compensated holidays, sick days and vacation, for example, are not hours worked and are therefore not counted in making overtime calculations.

B. Work week and Workday: Unless otherwise provided, for purposes of calculating overtime, each work week begins on Sunday and each workday begins at midnight.

## TIME RECORDS

Each department records the attendance of their employees. Our attendance records are Company records, and care must be exercised in recording the hours worked, overtime hours, and absences. Employees are not to clock or sign in or out for other employees. Violations of this policy may result in appropriate disciplinary action, up to and including immediate discharge.

Employees who work more than five hours per day will be provided with an unpaid lunch break of at least thirty minutes, and up to one hour (subject to your supervisor's approval on a daily basis). Non-exempt employees must clock in and out for lunch.

Once an employee clocks or signs in, work is to commence immediately. Failure to do so is considered falsification of timekeeping records.

If an employee forgets to clock or sign in or out, he or she must notify his or her supervisor immediately so the time may be accurately recorded for payroll.

An employee's supervisor must approve all overtime; employees with overtime without prior approval will be subject to disciplinary action.

Exempt employees are not required to sign in or out; however, business trips, vacation, sick, and bereavement, jury duty, or unpaid leave days must be approved and recorded.

## MEAL PERIODS

All employees working a shift lasting at between 6 and 10 hours in a workday are required to take an unpaid 30-minute meal break, sometime between the fourth and fifth hour of their shift. If you work a shift of more than 10 hours in a workday, you must take a second 30-minute meal break beginning before the end of the tenth hour of work. Non-exempt employees must clock out at the beginning of a meal period and clock back in when ending a meal period and returning to work.

The only circumstances in which a meal period may be waived are when you will not work more than six hours in a day and where you will complete your work for the day by not working more than six hours after the end of the last meal period and where you and the Company agree to waive the meal period. Any such waiver must be documented in advance in writing.

Please note that the failure to take a meal period will be considered as a violation of Company policy and will be treated as a performance issue.

## REST BREAKS

If you work a shift lasting more than 3 ½ hours, you are entitled to take a paid 10-minute rest break according to the following schedule:	<b>Number of Ten-Minute Rest Periods</b>
<b>Hours of Work In Day</b>	
0 up to 3.5	0
3.5 up to 6	1
6 up to 10	2
10 to 14 and so on for each additional four hours of work	3

You may not leave the premises of your place of work during rest breaks. The first rest break should be taken about halfway between starting time and your meal period. The second rest break should be taken about halfway between your meal period and the end of your shift. Do not clock out for rest breaks. If you are working a shift in excess of 10 hours in a workday, you are entitled to a third rest break. Your supervisor will schedule your meal and rest periods.

## LACTATION ACCOMMODATION

In recognition of the well-documented health advantages of breastfeeding for infants and mothers, the Company provides a supportive environment to enable breastfeeding mothers to express their breast milk during work hours. The Company will provide a reasonable amount of break time to accommodate an employee desiring to express breast milk for the employee's infant child. The break time, if possible, must run concurrently with rest and meal periods already provided to the employee. If the break time cannot run concurrently with rest and meal periods already provided to the employee, the break time will be unpaid. Where unpaid breaks or additional time are required, the employee will work with her supervisor regarding scheduling.

The Company will make reasonable efforts to provide employees with the use of a room or private location near the employee's work location, other than a toilet stall, for the employee to express milk. This location may be the employee's private office, if applicable. Employees should discuss with their supervisor, or any other member of management, or Human Resources representative the location to express their breast milk and for storage of expressed milk and to make any other arrangements under this policy. The Company may not be able to provide additional break time if doing so would seriously disrupt the Company's operations.

## PERSONNEL RECORDS

To keep necessary Company records up to date, it is extremely important that you notify the Human Resources Department of any changes in:

- Name and/or marital status
- Address and/or telephone number

- # Of eligible dependents
- W-4 deductions
- Person to contact in case of emergency

Changes to this information should be provided by the employee through the Human Resources Benefits on-line system.

## TIME OFF

### LEAVES OF ABSENCE

#### INTRODUCTION

For eligible employees, Telenav provides:

(1) family care and medical leave for up to 12 weeks per year in accordance with the California Family Rights Act ("CFRA") and the federal Family and Medical Leave Act of 1993 ("FMLA");

(2) pregnancy leave for up to four months in accordance with the California Fair Employment and Housing Act ("FEHA");

(3) disability leave as required to reasonably accommodate employees with a qualified disability under the Americans with Disabilities Act ("ADA"), the FEHA or any other federal, state or local law; and

(4) leave for other legally required absences and as permitted by the Company, including, but not necessarily limited to, those set forth below.

Employees having any questions regarding their right to take a leave should contact the Human Resource Manager. Telenav will provide employees with all leaves as required by federal, state or local laws.

### FAMILY CARE & MEDICAL LEAVE (CALIFORNIA FAMILY RIGHTS ACT LEAVE)

Telenav will grant family and medical leave in accordance with the requirements of applicable state and federal law in effect at the time the leave is granted. Although the federal and state laws sometimes have different names, the Company refers to these types of leaves collectively as either "Family Care and Medical Leave" or "FMLA Leave." No greater or lesser leave benefits will be granted than those set forth in such state or federal laws. In certain situations, the federal law requires that provisions of state law apply. In any case, employees will be eligible for the most generous benefits available under applicable law.

Please contact your supervisor as soon as you become aware of the need for a FMLA Leave. Employees are expected to provide prompt notice to the Company of any change(s) to an employee's return to work date. Accepting other employment, continuing to work in another job, or filing for unemployment insurance benefits while on leave may be treated as a voluntary resignation from employment, unless you and the Company have agreed, in writing, otherwise.

## A. EMPLOYEE ELIGIBILITY

To be eligible for FMLA Leave benefits, you must: (1) have worked for the Company for a total of at least 12 months; (2) have worked at least 1,250 hours over the previous 12 months as of the start of the leave; and (3) work at a location where at least 50 employees are employed by the Company within 75 miles, as of the date the leave is requested.

## B. REASONS FOR LEAVE

State and federal laws allow FMLA Leave for various reasons. Because an employee's rights and obligations may vary depending upon the reason for the FMLA Leave, it is important to identify the purpose or reason for the leave. FMLA Leave may be used for one of the following reasons:

(1) the birth, adoption, or foster care of an employee's child within 12 months following birth or placement of the child ("Bonding Leave");

(2) to care for an immediate family member (spouse, registered domestic partner, child, or parent with a serious health condition ("Family Care Leave"));

(3) an employee's inability to work because of a serious health condition ("Serious Health Condition Leave");

(4) a "qualifying exigency," as defined under the FMLA, which essentially means attending to certain activities to prepare for a spouse's, registered domestic partner's, child's, or parent's active duty or call to active duty in a foreign country as a member of the military reserves or National Guard or Armed Forces ("Military Emergency Leave"); or

(5) to care for a spouse, child, parent or next of kin (nearest blood relative)—who is (a) an Armed Forces member (including the military reserves and National Guard) undergoing medical treatment, recuperation, or therapy, is otherwise in an outpatient status, or is otherwise on the temporary disability retired list—with a serious injury or illness incurred or aggravated in the line of duty while on active duty that may render the individual medically unfit to perform his or her military duties; or (b) a person who, during the five (5) years prior to the treatment necessitating the leave, served in the active military, Naval, or Air Service, and who was discharged or released therefrom under conditions other than dishonorable (a "veteran" as defined by the Department of Veteran Affairs) and who has a serious injury or illness incurred or aggravated in the line of duty while on active duty that manifested itself before or after the member became a veteran ("Military Caregiver Leave").

## C. LENGTH OF LEAVE

The maximum amount of FMLA Leave will be twelve (12) workweeks in any 12-month period when the leave is taken for: (1) Bonding Leave; (2) Family Care Leave; (3) Serious Health Condition Leave; and/or (4) Military Emergency Leave. However, if both spouses (or registered domestic partners) work for the Company and are eligible for leave under this policy, the spouses (or registered domestic partners) will be limited to a total of 12 workweeks off between the two of them when the leave is for Bonding Leave. **A 12-month period begins on the date of your first use of FMLA Leave. Successive 12-**

**month periods commence on the date of your first use of such leave after the preceding 12-month period has ended.**

The maximum amount of FMLA Leave for an employee wishing to take Military Caregiver Leave will be a combined leave total of twenty-six (26) workweeks in a single 12-month period. A "single 12-month period" begins on the date of your first use of such leave and ends 12 months after that date.

If both spouses work for the Company and are eligible for leave under this policy, the spouses will be limited to a total of 26 workweeks off between the two when the leave is for Military Caregiver Leave only or is for a combination of Military Caregiver Leave, Military Emergency Leave, Bonding Leave and/or Family Care Leave taken to care for a parent.

Under some circumstances, you may take FMLA Leave intermittently, which means taking leave in blocks of time, or by reducing your normal weekly or daily work schedule.

To the extent required by law, some extensions to FMLA Leave may be granted when the leave is necessitated by a pregnancy related disability or a "disability" as defined under the Americans with Disabilities Act, the California Fair Employment and Housing Act and/or other applicable federal, state or local law. In addition, in some circumstances and in accordance with applicable law, an extension to FMLA Leave may be granted when the leave is taken to care for a registered domestic partner and/or a registered domestic partner's child. Certain restrictions on these benefits may apply.

## D. NOTICE AND CERTIFICATION

(i) Bonding, Family Care, Serious Health Condition, and Military Caregiver Leave Requirements

Employees are required to provide:

1. when the need for the leave is foreseeable, 30 days prior notice or such notice as is both possible and practical if the leave must begin in less than 30 days (normally this should be the same day the employee becomes aware of the need for leave or the next business day);

2. when the need for leave is not foreseeable, notice within the time prescribed by the Company's normal absence reporting policy, unless unusual circumstances prevent compliance, in which case notice is required as soon as is otherwise possible and practical;

3. when the leave relates to medical issues, a completed Certification of Health-Care Provider form within 15 calendar days (for Military Caregiver Leave, an invitational travel order or invitation travel authorization may be submitted in lieu of a Certification of Health-Care Provider form);

4. periodic recertification (upon request); and

5. periodic reports during the leave.

Certification forms are available from the Human Resources Department. At the Company's expense, the Company may also require a second or third medical opinion regarding your own serious health condition. Employees are expected to cooperate

with the Company in obtaining additional medical opinions that the Company may require.

When leave is for planned medical treatment, you must try to schedule treatment so as not to unduly disrupt the Company's operation. Please contact the Human Resources Department prior to scheduling planned medical treatment.

#### (ii) Military Emergency Leave

Employees are required to provide:

1. as much prior notice as is reasonable and practicable under the circumstances;
2. a copy of the covered military member's active duty orders when the employee requests leave; and
3. a completed Certification of Qualifying Exigency form within 15 calendar days, unless unusual circumstances exist to justify providing the form at a later date.

Certification forms are available from the Human Resources Department.

#### (iii) Failure to Provide Certification and to Return from Leave

Absent unusual circumstances, failure to comply with these notice and certification requirements may result in a delay or denial of the leave. If you fail to return to work at your leave's expiration and have not obtained an extension of the leave, the Company may presume that you do not plan to return to work and may voluntarily terminate your employment.

### E. COMPENSATION DURING LEAVE

Generally, FMLA Leave is unpaid. However, you may be eligible to receive benefits through State-sponsored or Company-sponsored wage-replacement benefit programs. If you are eligible to receive these benefits, you may also choose to supplement these benefits with the use of accrued vacation and sick leave, to the extent permitted by law and Company policy. All such payments will be integrated so that you will receive no more than your regular compensation during this period. If you are not eligible to receive any of these wage-replacement benefits, the Company may require you to use accrued vacation and sick leave to cover some or all of the FMLA Leave, to the extent permissible by law. The use of paid benefits will not extend the length of a FMLA Leave.

### F. BENEFITS DURING LEAVE

The Company will continue making contributions for your group health benefits during your leave on the same terms as if you had continued to work. This means that if you want your benefits coverage to continue during your leave, you must also continue to make any premium payments that you are now required to make for yourself or your dependents. Employees taking Bonding Leave, Family Care Leave, Serious Health Condition Leave, and Military Emergency Leave will generally be provided with group health benefits for a 12-work week period. Employees taking Military Caregiver Leave may be eligible to receive group health benefits coverage for up to a maximum of 26 workweeks. In some

instances, the Company may recover premiums it paid to maintain health coverage if you fail to return to work following a FMLA Leave.

If you are on a FMLA Leave but are not entitled to continued paid group health insurance coverage, you may continue your coverage through the Company in conjunction with federal and/or state COBRA guidelines by making monthly payments to the Company for the amount of the relevant premium. Please contact the Human Resources Department for further information.

Your length of service as of the leave will remain intact, but accrued benefits such as vacation and sick leave will not accrue while on an unpaid FMLA Leave.

### G. JOB REINSTATEMENT

Under most circumstances, you will be reinstated to the same position held at the time of the leave or to an equivalent position with equivalent pay, benefits, and other employment terms and conditions. However, you have no greater right to reinstatement than if you had been continuously employed rather than on leave. For example, if you would have been laid off had you not gone on leave, or if your position has been eliminated during the leave, then you will not be entitled to reinstatement.

Prior to being allowed to return to work, an employee wishing to return from a Serious Health Condition Leave must submit an acceptable release from a health care provider that certifies the employee can perform the essential functions of the job as those essential functions relate to the employee's serious health condition. For an employee on intermittent FMLA Leave, such a release may be required if reasonable safety concerns exist regarding the employee's ability to perform his or her duties, based on the serious health condition for which the employee took the intermittent leave.

"Key employees," as defined by law, may be subject to reinstatement limitations in some circumstances. If you are a "key employee," you will be notified of the possible limitations on reinstatement at the time you request a leave.

A Notice to Employees Of Rights Under FMLA is attached to this handbook.

## PREGNANCY DISABILITY LEAVE

### Leave Entitlement

Any employee who is *actually disabled* by pregnancy, childbirth, or a related medical condition is eligible for a Pregnancy Disability Leave of Absence. There is no length of service requirement.

For purposes of this policy, you are *actually disabled* when, in the opinion of your healthcare provider, you cannot work at all or are unable to perform any one or more of the essential functions of your job or to perform them without undue risk to yourself, the successful completion of your pregnancy, or to other persons as determined by a health care provider. This term also applies to severe morning sickness or if you need to take time off for prenatal care.

## TRANSFER TO LESS STRENUOUS POSITION

The Company will transfer an employee *affected by pregnancy* to a less strenuous or hazardous position or duties if:

She requests a transfer;

The request is based upon the certification of her health care provider as “medically advisable”; *and*

The transfer can be reasonably accommodated.

You are *affected by pregnancy* if you are pregnant or have a related medical condition, and because of pregnancy, your health care provider has certified that it is medically advisable for you to transfer. No additional position will be created and the Company will not discharge another employee, transfer another employee with more seniority or promote or transfer any employee who is not qualified to perform the new job.

## PRIOR NOTICE AND MEDICAL CERTIFICATION

As a condition of a pregnancy disability leave of absence or a transfer, you must:

Provide 30 days’ notice before the leave of absence or transfer is to begin, if the need for the leave of absence or transfer is foreseeable, or when 30 days’ notice is not foreseeable, as soon as practicable; and

Provide a signed medical certification from your health care provider, that states that you are disabled due to pregnancy or that it is medically advisable for you to be transferred to a less strenuous or hazardous position or to less strenuous or hazardous duties.

The Company may require you to provide a new certification if you request an extension of your leave of absence.

## DURATION OF THE LEAVE OF ABSENCE

A Pregnancy Disability Leave of Absence will last for the duration of your pregnancy-related disability as certified by your health care provider for up to four (4) months. Leave is available for all disabilities related to each pregnancy and does not need to be taken in one continuous period.

## RETURN TO WORK

If you and the Company have agreed upon a definite date of return from your leave of absence or transfer, you will be reinstated on that date if you notify the Company that you are able to return on that date. If the length of the leave of absence or transfer has not been established, or if it differs from the original agreement, you will return to work within two (2) business days, where feasible, after you notify the Company of your readiness to return.

Before you will be allowed to return to work following a leave of absence or transfer, you must provide your supervisor with a certification from your health care provider that you can perform safely all of the essential duties of your position, with or without reasonable accommodation. If you do not provide such a release prior to or upon reporting for work,

you will be sent home until a release is provided. This time before the release is provided will be unpaid.

You will be returned to the same position or duties upon the conclusion of your leave of absence or transfer unless:

- You would not otherwise have been employed in the same position at the time you request reinstatement for legitimate business reasons unrelated to the leave of absence; or
- Each means of preserving your job or duties would have substantially undermined the Company’s ability to operate the business safely and efficiently.

If the Company cannot return you to your original job, it will offer you a comparable position provided that one exists and is available. However, an employee will not be entitled to any greater right to reinstatement than if that employee had not taken the leave. For example, if an employee would have been laid off regardless of the leave, and there is no equivalent position available upon return from leave, then the employee will not be entitled to reinstatement. Additionally, if the Company is unable to keep the employee’s position open because to do so would undermine the safe and efficient operations of the Company, and if there is no equivalent position available at the time of the employee’s return, reinstatement will be denied.

Failure to return to work after the leave of absence may result in termination of employment.

## INTEGRATION WITH OTHER BENEFITS.

Pregnancy Disability Leaves of Absence are unpaid. You may elect to use accrued sick leave and/or accrued vacation benefits during the unpaid leave of absence. However, use of paid time off will not extend the available leave of absence time. Vacation and sick leave hours will not accrue during any unpaid portion of the leave of absence, and you will not receive pay for official holidays that are observed during your leave of absence except during those periods when you are substituting vacation or sick leave for unpaid leave.

Employees should apply for California State Disability insurance (“SDI”) benefits. SDI forms are available from the Company or your health care provider. Any SDI for which you are eligible will be integrated with accrued vacation, sick leave, or other paid time off benefits so that you do not receive more than 100% of your regular pay.

## OTHER DISABILITY LEAVES

In addition to FMLA and pregnancy disability leaves as described above, otherwise qualified employees may take a temporary disability leave of absence if necessary to reasonably accommodate a disability under the ADA, the FEHA or any other federal, state or local laws and the leave will not create undue hardship for the Company. Any disability leave under this section will run concurrently with any FMLA or pregnancy disability leave to which the employee is entitled under Company policy or applicable laws.

Disability leaves under this section will be unpaid, except that employees may be required to use any

accrued sick leave and may be allowed to use accrued vacation time before taking unpaid leave.

Employees taking disability leave must comply with the Family Care and Medical Leave provisions regarding substitution of paid leaves notice and medical certification. For the purpose of applying these provisions, a disability leave will be considered to be a medical leave.

If a disability leave under this section extends beyond 12 weeks in a 12-month period, and the employee was receiving continued employer contributions toward any employee benefit plan, the employee will not be entitled to any continued employer contributions towards any employee benefit plan unless otherwise required by law. An employee, however, may elect to continue participating in such benefit plans, at the employee's own expense, to the extent permitted by such plans.

The duration of a leave under this section shall be consistent with applicable law, but in no event shall the leave extend past the date on which an employee is cleared by his/her doctor to return to work and is capable of performing the essential functions of his or her position, with or without reasonable accommodation. For a full explanation of leave duration and reinstatement rights, employees should contact the Human Resources Department.

### **OTHER LEAVES OF ABSENCE**

Telenav also grants eligible employees leaves of absence for various reasons under Company policy and/or as may be required by federal, state or local laws. Unless otherwise required by law, employees will not be paid for such leaves of absence.

The leaves available to employees may change. Employees wishing to take a leave of absence should contact the Human Resource Department for more information on the leaves available to employees, the eligibility requirements for the leaves and the procedures for taking the leave.

### **MILITARY LEAVE**

Both state and federal law provide employees with the right to take leave to serve in the military. At the federal level, the Uniformed Services Employment and Reemployment Rights Act, commonly referred to as "USERRA", governs military leave rights. In addition to the federal protections under USERRA, employees in California who serve in the military are entitled to the rights and protections set forth in the California Military and Veteran's Code. Among other things, the Code prohibits discrimination against members of the military or naval services of the state or the United States, and grants members of the National Guard or U.S. Reserve a temporary leave of absence while engaged in military duty ordered for purposes of military training, drills, encampment, naval cruises, and special exercises or like activities. This leave is not to exceed 17 calendar days annually.

### **ELIGIBILITY FOR LEAVE**

Telenav provides unpaid military leaves of absence to employees who serve in the uniformed services as required by USERRA and applicable state laws. The uniformed services include the Army, Navy, Marine Corps, Air Force, Coast Guard, Army

National Guard, Air National Guard, Commissioned Corps of the Public Health Service and any other category of persons designated by the President of the United States in time of war or emergency. The uniformed services also include participants in the National Disaster Medical System ("NDMS") when activated to aid in response to a public health emergency or to be present for a short period when there is a risk of public health emergency, or when they are participants in authorized training.

Service consists of the performance of any of the following on a voluntary or involuntary basis: active duty, active duty for training, initial active duty, inactive duty training, full-time National Guard duty and absence from work for an examination to determine fitness for such duty. Total military leave time may not exceed five years during employment, except in special circumstances.

### **NOTICE OF LEAVE**

Prior notice of leave is required, preferably in writing. Please provide your supervisor with as much notice as possible of any anticipated leave of absence for military duty or training.

### **SALARY AND BENEFITS DURING LEAVE**

Military leave is unpaid. Any accrued vacation will be paid during military leave at your request. Employees on military leave may elect to continue their health plan coverage at their own expense for up to 24 months or during service, whichever is shorter.

### **REINSTATEMENT**

To be eligible for reinstatement, the employee must have provided prior notice of the military obligation and have completed his or her service honorably. Employees who are absent from work 30 days or less or who are absent to take a fitness exam must report to work at the beginning of the first regularly scheduled work day following completion of service, after allowing for the safe travel home and 8 hours of rest. If the employee serves 31 to 180 days, he or she must apply for reemployment within 14 days after completing service. If the employee has served 181 days or more, he or she must apply for reemployment within 90 days after completing service.

As with other leaves of absence, failure to return to work or to reapply within applicable time limits may result in loss of reemployment rights. Temporary employees may not be eligible for reinstatement following military leave and reinstatement may not be required for other employees in some circumstances. Full details regarding reinstatement are available from the Human Resources Department.

In general, an employee returning from military leave will be reemployed in the position and seniority level that the employee would have attained had there been no military leave of absence. If necessary, the Company will provide training to assist the employee in the transition back to the workforce.

An employee returning from military leave is entitled to any unused, accrued vacation benefits the employee had at the time the military leave began.

Upon reinstatement, the employee will accrue vacation benefits at the rate he or she would have attained if no military leave had been taken.

## **FAMILY MILITARY LEAVE**

Employees who are spouses of certain military personnel may receive up to ten (10) days of unpaid leave during a qualified leave period. For purposes of this policy, a "qualified leave period" means the period during which the individual is on leave from deployment during a period of military conflict.

An employee is eligible for leave under this policy if he or she:

1. Is the spouse of a person who: (s) is a member of the Armed Forces of the United States who has been deployed during a period of military conflict to an area designated as a combat theater or combat zone by the President of the United States, or (b) is a member of the National Guard or of the Reserves who has been deployed during a period of military conflict;
2. Works for an average of 20 or more hours per week;
3. Provides notice of his or her intention to take leave within two business days of receiving notice that his or her spouse will be on leave from deployment; and
4. Submits written documentation certifying that their spouse will be on leave from deployment during the time the leave is requested.

Military conflict means either a period of war declared by the United States Congress, or a period of deployment for which a member of a reserve component is ordered to active duty either by the Governor or the President of the United States.

Leave taken under this policy will not affect an employee's right to any other benefits, although an employee may elect to use accrued paid time off during the leave.

Telenav will not discriminate against, or tolerate discrimination against, any employee who requests and/or takes leave under this policy.

For more information, please contact your supervisor or the Human Resources Department.

## **TIME OFF FOR VOLUNTEER FIREFIGHTERS, RESERVE PEACE OFFICERS OR EMERGENCY RESCUE PERSONNEL.**

If you are a registered volunteer firefighter, reserve peace officer, or emergency rescue personnel who intends to perform emergency duty during work hours, please alert your supervisor so the Company is aware of the fact that the employee may have to take time off to perform emergency duty. In the event any employee needs to take time off for this type of emergency duty, a supervisor must be notified before leaving work. All time off for these purposes is unpaid.

Registered volunteer firefighters, reserve peace officers or emergency rescue personnel are eligible to take temporary unpaid leaves of absence for fire

or law enforcement training not to exceed 14 days per calendar year.

## **CIVIL AIR PATROL LEAVE**

Telenav will not discriminate against an employee for membership in the Civil Air Patrol. Additionally, the Company will not retaliate against an employee for requesting or taking Civil Air Patrol leave.

Telenav will provide not less than 10 days per year of leave but no more than 3 days at a time to employees who are volunteer members of the Civil Air Patrol. Employees must have been employed by the Company for at least 90 days immediately preceding the commencement of leave, and must be duly directed and authorized by a political entity that has the authority to authorize an emergency operational mission of the Air Patrol.

Employees must request leave with as much notice as possible before responding to an emergency operational mission of the Civil Air Patrol.

Leave under this policy is unpaid. An employee taking leave under this policy will not be required to exhaust accrued vacation, personal leave, sick leave or any other type of accrued leave prior to taking unpaid Civil Air Patrol Leave.

Following leave under this policy, an employee must return to work as soon as practicable and must provide evidence of the satisfactory completion of Civil Air Patrol service. If the employee complies with these requirements, the employee will be restored to their prior position without loss of status, pay, or other benefits.

## **TIME OFF FOR BONE MARROW DONATION**

Employees will be provided a leave of absence to undergo a medical procedure to donate bone marrow to another person. The combined length of bone marrow leave may not exceed five workdays in any one-year period. To qualify for this leave, the employee must submit verification by a physician detailing that there is a medical necessity for the donation, as well as the length of each leave requested. Employees must use earned sick/vacation time concurrently with this time off. If an employee does not have enough earned sick/vacation time to cover the leave, the remaining days of leave will be with pay by the Company. Use of this leave will not be counted against any available FMLA/CFRA time. This is also not considered a break in service for purposes of benefits or seniority.

While on leave for bone marrow donation, the Company will maintain all group health insurance benefits as if the employee was still at work.

In most circumstances, upon return from this leave, an employee will be reinstated to his/her original job or to an equivalent job with equivalent pay, benefits, and other employment terms and conditions. However, an employee has no greater right to reinstatement than if he/she did not take a leave. For example, if an employee on leave for bone marrow donation would have been laid off had he/she not taken a leave, or if the employee's job is eliminated during the leave and no equivalent or comparable job is available, then the employee would not be entitled to reinstatement.

## TIME OFF FOR ORGAN DONATION

Employees will be provided a leave of absence to undergo a medical procedure to donate an organ to another person. The combined length of the leaves may not exceed 30 days in any one-year period. To qualify for this leave, the employee must submit verification by a physician detailing that there is a medical necessity for the donation, as well as the length of each leave requested. If the leave is for two weeks or less, employees must use all available sick/vacation time concurrently with this time off. If an employee does not have enough available accrued sick/vacation time, then any remaining days of leave will be with pay by the Company. If the leave is more than two weeks, employees must use their available sick/vacation time during the first two weeks, and the remaining days of leave will be with pay by the Company. Use of this leave will not be counted against any available FMLA/CFRA time. This is also not considered a break in continuous service for purposes of benefits or seniority.

While on leave for organ donation, the Company will maintain all group health insurance benefits as if the employee was still at work.

In most circumstances, upon return from this leave, an employee will be reinstated to his/her original job or to an equivalent job with equivalent pay, benefits, and other employment terms and conditions. However, an employee has no greater right to reinstatement than if he/she did not take a leave. For example, if an employee on leave for organ donation would have been laid off had he/she not take a leave, or if the employee's job is eliminated during the leave and no equivalent or comparable job is available, then the employee would not be entitled to reinstatement.

## TIME OFF FOR DOMESTIC VIOLENCE VICTIMS

Telenav will provide time off to any employee who is a victim of domestic violence and/or a victim of sexual assault so that the employee may obtain or attempt to obtain relief and to help ensure the health, safety, or welfare of the employee or the employee's child. The relief that may be sought includes, but is not limited to, a temporary restraining order, restraining order, or other injunctive relief. When taking such leave, the employee should give the Company reasonable notice of the leave, unless prior notice is not feasible. The Company also may require the employee to provide written verification of the need for the time off, such as a police report, court order or documentation from a medical professional, etc.

Additionally, an employee who is a victim of domestic violence and/or a victim of sexual assault may take time off to attend to any of the following: (1) to seek medical attention for injuries caused by domestic violence; (2) to obtain service from a domestic violence shelter, program, or rape crisis center; (3) to obtain psychological counseling; and (4) to participate in safety planning and to take other actions to increase safety from future domestic violence or sexual assault, including temporary or permanent relocation.

Confidentiality of the situation, including the employee's request for the time off, will be maintained to the greatest extent possible. Employees may use accrued benefits, such as

existing vacation time or other accrued paid time off, in order to receive compensation during the time taken off from work.

## TIME OFF FOR VICTIMS OF CRIME

Telenav prohibits discrimination against an employee who wishes to take time off from work to attending judicial proceedings related to certain crimes committed against the employee, the employee's immediate family member, the employee's registered domestic partner, or a child of the employee's domestic partner. Employees are eligible to take time off for crimes including: a violent felony, as defined in subdivision (c) of Section 667.5 of the Penal Code; a serious felony, as defined in subdivision (c) of Section 1192.7 of the Penal Code; and a felony provision of law proscribing theft or embezzlement.

Before an employee may be absent from work for this purpose, the employee must provide his or her supervisor with a copy of the notice of each scheduled proceeding that is provided to the victim by the agency responsible for providing notice, unless prior notice is not feasible. If an unscheduled judicial proceeding occurs, which requires your immediate absence, please alert your supervisor before leaving Company premises. The Company may require that the employee provide verification that the absence from work was due to attendance at the unscheduled judicial proceeding. The types of verification the Company may require include documentation evidencing the judicial proceeding from any of the following entities: the court or government agency setting the hearing; the district attorney or prosecuting attorney's office; or the victim/witness office that is advocating on behalf of the victim.

Confidentiality of the situation, including the employee's request for the time off, will be maintained to the greatest extent possible if an employee requests time off for these reasons. Employees may use accrued benefits, such as existing vacation time or other accrued paid time off, in order to receive compensation during the time taken off from work.

For purposes of this policy, immediate family member is defined as an employee's spouse, child, stepchild, brother, stepbrother, sister, stepsister, mother, stepmother, father, or stepfather.

## JURY & WITNESS DUTY

Telenav will provide employees time off to serve, as required by law, on a jury or grand jury if the employee provides reasonable prior notice. Telenav will also provide employees with time off to appear in court or other judicial proceedings as a witness to comply with a valid subpoena or other court order.

Employees will be granted a paid leave of absence of up to five

(5) business days per year for fulfilling jury duty. Any jury duty that extends beyond (5) business days per year will be unpaid.

However, exempt employees who work any portion of a workweek in which they also serve on jury duty or appear as a witness will receive their full salary for that workweek. Employees may elect to substitute

accrued vacation during any unpaid leave due to jury duty or a witness appearance.

Employees are required to provide reasonable prior notice of the need for jury/witness leave.

## LEAVE FOR EDUCATIONAL/DAYCARE PURPOSES

Employees will be granted time off without pay for up to 40 hours per calendar year, but no more than eight hours in any calendar month, to participate in the activities of schools or licensed child daycare facilities attended by their children. Employees must substitute accrued vacation time off for purposes of a planned absence under this Section.

You also may be granted time off to attend a school conference involving the possible suspension of your child. Please contact your supervisor if time off is needed for this reason.

Employees wishing to take time off under this Section must provide their supervisors with reasonable notice of the planned absence. If both parents of a child are employed by Telenav at the same worksite, the request for time off under this Section will be granted to the first parent to provide notice of the need for time off. The request from the second parent will be accommodated if possible.

Telenav reserves the right to request that the employee furnish written verification from the school or daycare facility as proof that the employee participated in school or daycare activities on the specific date and time. Failure to provide written verification is grounds for disciplinary action.

## VOTING TIME OFF

Employees who do not have sufficient time outside of their regular working hours to vote in a statewide election may request time off to vote. If possible, employees should make their request at least two workdays in advance of the election. Up to two hours of paid time off will be provided, at the beginning or end of the employee's regular shift, whichever will allow the greatest amount of free time for voting and the least time off work. Any additional time off will be without pay.

## BEREAVEMENT LEAVE

### IMMEDIATE FAMILY

All full time regular employees will be eligible for payment for absence due to the death of a member of their immediate family. Full time employees are paid for time absent from scheduled work **on the day of death through the day after the funeral**, but not to exceed 5 calendar days.

#### Immediate family includes:

- Mother or Stepmother
- Mother-in-law
- Father or Stepfather
- Father-in-law
- Sister or Stepsister
- Brother or Stepbrother
- Wife or Husband
- Child or Stepchild
- Daughter-in-law

- Son-in-law
- Grandparent or Step-grandparent
- Grandchild or Step-grandchild
- Great Grandparent
- Great Grandchild
- Domestic Partner
- Mother or Stepmother of domestic partner
- Father or Stepfather of domestic partner
- Child or stepchild of domestic partner
- Daughter-in-law of domestic partner
- Son-in-law of domestic partner
- Any family member living with the employee at the time of the family member's death

### NON-IMMEDIATE FAMILY

All employees are eligible for payment for time absent from scheduled work **the day of the funeral** for a non-immediate family member.

#### NON-IMMEDIATE FAMILY INCLUDES:

- Brother-in-law
- Sister-in-law
- Aunt or Uncle of employee or spouse
- Niece or Nephew of employee or spouse
- First cousin of employee
- Grandparents of spouse
- Great Grandparents of spouse
- Brother-in-law of domestic partner
- Aunt or uncle of domestic partner
- Grandparents of domestic partner
- Great-Grandparents of domestic partner

Any additional time off may be permitted, but will be unpaid. Employees who obtain approval for additional bereavement leave may use any accrued vacation for the otherwise unpaid period of leave.

## SICK LEAVE

Telenav full time, regular employees are given 10 paid sick days per calendar year to protect them in times of illness. The 10 days are granted to the eligible employee each January 1<sup>st</sup>. Eligible employees who are hired in any month after January will receive a prorated number of sick days. Any eligible employee hired after August 30<sup>th</sup> of any given year will receive 5 paid sick days for the remainder of that calendar year. Part time and temporary employees are not eligible to earn sick leave. Sick leave may be taken for the employee's personal illness, medical emergency, or disability. Hours absent for medical and dental appointments will be treated as sick leave for non-exempt employees. An employee may also take up to one-half of his/her sick leave entitlement for a year to attend to an illness of his/her child, parent, spouse, or registered domestic partner. "Child" means a biological, foster or adopted child, a stepchild, a legal ward, a child of a registered domestic partner, or a child of a person standing in loco parentis.

To be eligible for sick pay, employees unable to report to work due to illness must notify their supervisor directly, each day of their absence, as far in advance as possible. If their supervisor is not available, the Human Resources Department should be contacted. If an employee is unable to personally notify his/her supervisor or HR, a family member or a friend should contact the supervisor. The supervisor or Human Resources must be contacted each day of absence.

If Telenav has questions about the nature or length of an employee's illness, a written certification from a physician or licensed health care professional may be required. When verifications are requested, such verifications and releases may be a condition to receiving sick leave benefits or returning to work. Although a health care certification normally will not be requested for absences of less than three working days, the Company may request such a statement where circumstances warrant.

Sick leave is paid at the employee's regular base rate of pay and is not counted for purposes of calculating "hours worked" for overtime purposes.

Unused sick leave may not be carried over to the next calendar year and is not paid out at the termination of employment.

## HOLIDAYS

The Company observes the following standard holidays each year:

- New Year's Day
- Presidents' Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Friday after Thanksgiving
- Christmas Eve Day
- Christmas Day
- New Year's Eve Day
- One floating holiday (chosen by the Company at the beginning of each year)

Eligible employees will receive a paid day off on each of the holidays listed above.

## ELIGIBILITY

Unless otherwise provided in this policy, all full-time employees will receive time off with pay at their normal base rate for each company-observed holiday. Part-time and temporary employees are not eligible for paid holiday benefits. Moreover, all employees are ineligible for holiday benefits that accrue while on leave of absence.

If a holiday falls on a Saturday or Sunday it will be observed consistent with public observance of the holiday. If you are asked to work on a holiday, you will be paid at your regular rate for the hours worked and arrangements will be made to allow you the flexibility to take alternative paid time off.

Holiday pay is given to eligible employees who are scheduled to work the day on which the holiday is observed. To receive holiday pay, the employee must work the scheduled working days immediately preceding and immediately following the holiday, unless an absence on either day is approved in advance by the supervisor or the employee receives supervisory approval following the absence based on a physician's statement.

Holiday pay is paid at the employee's regular base rate of pay and is not counted for purposes of calculating "hours worked" for overtime purposes.

## VACATION POLICY

Telenav provides vacation benefits to eligible employees to enable them to take paid time off for rest and recreation. Telenav believes that this time is valuable for employees to enhance their productivity and to make their work experience with the Company personally satisfying. Telenav also provides long-service employees with additional vacation benefits as years of service are accumulated.

## VACATION ACCRUAL

All regular full-time employees are eligible to accrue vacation benefits based on their continuous length of service, measured from the date of hire. "Continuous length of service" is defined as service that is uninterrupted by discharge of employment and subsequent rehire by Telenav or a break in service that has been bridged. Employees accrue vacation each pay period, unless they have reached their accrual cap as specified below or as otherwise required by applicable law.

- Employees with 0-5 years of service: accrue 15 days per year, max accrual cap of 160 hours
- Employees with 5-10 years of service: accrue 20 days per year, max accrual cap of 200 hours
- Employees with 10+ years of service: accrue 25 days per year, max accrual cap of 240 hours

Telenav's Human Resources Benefit self service module, through Ultimate Software (Ultipro), or its successor system, will allow employees to log on and see how much time off they have accrued at a given time of the year.

Vacation accruals continue up to a maximum ("accrual cap"). If an employee reaches his/her accrual cap, then that employee shall not accrue any additional vacation until he/she uses a portion of vacation previously accrued. Additionally, no retroactive accrual or payment will be permitted for this period. Once an employee uses vacation to get below the accrual cap, the employee will start to accrue vacation again until the accrual cap is reached.

No vacation accrues during an unpaid leave of absence or while on disability salary continuation. Vacation accruals recommence when the employee returns to work.

Vacation pay will be at the employee's current base salary (not including any commissions or bonus pay to which the employee may be eligible). Vacation time taken will not be considered as time worked for purposes of calculating overtime. Vacation time must be recorded properly in the HR Benefits on line system.

## VACATION PAY ON DISCHARGE

When employment ends, the employee is paid all accrued but unused vacation at the employee's base rate of pay at the time he or she leaves the Company.

## **VACATION APPROVAL**

All vacations must be approved in advance by the employee's immediate supervisor through Telenav's HR Benefits on line self-service request system.

## **VACATION SCHEDULING**

Scheduling of vacations is to be done in a manner consistent with Telenav's operational requirements. Vacation requests should be submitted by employees to their immediate supervisor for approval at least two weeks prior to the commencement of a vacation period through automated HR Benefits on line self service requests. If two or more employees have requested vacations covering the same period and may not be absent simultaneously, preference shall be given to the employee with the greater length of service. Subject to supervisor approval, an employee may otherwise schedule and take vacation at any time once it has accrued.

## **HOLIDAYS OCCURRING DURING VACATION**

If an observed Telenav holiday occurs during an employee's scheduled vacation, no deduction from accrued vacation will be made for the holiday period. An employee may add to his or her vacation period by adding to or using the holiday period in place of accrued vacation time.

## **VACATION DURING HOLIDAY SHUTDOWN**

At its discretion, the Company may schedule a US Companywide Shutdown during one or more holiday periods. During these periods, employees will be required to use their vacation days to cover any days during the shutdown that are not Company holidays. Employees without accrued vacation days may opt to take unpaid days off for those days. Employees who have a compelling need to work during such a Shutdown should seek the prior approval of their manager and notify HR. The Company has scheduled such Shutdown periods annually since 2014.

## **VACATION FOR FAMILY CARE AND MEDICAL LEAVE PURPOSE**

Employees who request family care or medical leave pursuant to Telenav's Family Care and Medical Leave policy must apply any available vacation pay balance to their family or medical leave to the extent permitted by the applicable laws.

## **BENEFITS OVERVIEW**

- **Medical**
- **Dental/Vision**
- **Life Insurance**
- **STD/LTD**
- **401K with Company Match**
- **FSA (Medical- Dependent Care)**
- **Direct Deposit**

Please refer to the summary plan or plan for these benefits for more information on the terms and coverage of these benefits. Also, the Human Resources Department has more information on these benefits.

## **ON THE JOB**

### **SEMINARS, PROFESSIONAL, CERTIFICATIONS AND RELATED MEMBERSHIP DUES**

Attendance at seminars and professional events helps Telenav employee's stay abreast of the latest technological, legal and experiential developments in their fields. Reimbursement of fees related to achievement of professional certifications (i.e., CPA, PHR, etc.) and related accredited membership is permitted, including related exam fees, upon prior approval of the Company. Education and seminar costs directly and specifically related to your existing job description and scope of work are reimbursable. Tuition for higher education is NOT reimbursable. All such costs are reimbursable ONLY if approved in ADVANCE by a Vice President and Director of Human Resources. Before attending any seminars or professional events or enrolling in any education program or seminar, please contact Human Resources to determine if the costs will be reimbursed and to get approval for the costs.

### **ATTENDANCE, PUNCTUALITY AND DEPENDABILITY**

Because Telenav depends heavily upon its employees, it is important that employees attend work as scheduled. Dependability, attendance, punctuality, and a commitment to do the job right are essential at all times. As such, employees are expected at work on all scheduled workdays and during all scheduled work hours and to report to work on time. Moreover, an employee must notify his/her supervisor or the Human Resources Department as far in advance as possible. This policy applies for each day of his/her absence. An employee who fails to contact his/her immediate supervisor or the Human Resources Department may be considered as having voluntarily resigned. A careful record of absenteeism and lateness is kept by the employee's supervisor and becomes part of the personnel record. To the extent permitted by law, absenteeism and lateness lessen an employee's chances for advancement and may result in dismissal.

### **WORK FROM HOME**

In certain instances, an employee may be granted approval to work from their home from their direct supervisor, depending on their position and work assignments. Work from home situations will be made on a case-by-case basis as part of an employees work agreement with their direct supervisor, and with approval from the Department Head. All work from home arrangements will be reevaluated on at least an annual basis. If prior arrangements have not been made for an employee to work from home, yet a situation arises where an employee would like to request approval for a particular reason, they may request so in writing to their direct supervisor with minimum 2 days advance notice. Ultimate discretion is left to the employee's Direct Supervisor and Department Head.

## DRUGS & DRUG ABUSE

Manufacture, distribution, dispensation, possession, or use of any illegal drug or controlled substance while on Company premises is **strictly prohibited**. These activities constitute serious violations of Company rules, jeopardize the Company and can create situations that are unsafe or that substantially interfere with job performance. Employees in violation of the policy are subject to appropriate disciplinary action, up to and including discharge. Additionally, Telenav reserves the right to require an employee to undergo a medical evaluation or drug test under appropriate circumstances.

Any employee suspected of possessing illegal drugs and/or controlled substances is subject to reasonable inspection and search, with or without notice. Employee's personal belongings, including any bags, purses, briefcases and clothing and all Company property, are also subject to reasonable inspection and search, with or without notice. Employees who violate the Company's Drug Abuse policy will be removed from the workplace immediately. The Company may bring the matter to the attention of appropriate law enforcement authorities. Any conviction for criminal conduct involving illegal drugs, intoxicants, or controlled substances, whether on or off duty, or any violation of the Company's drug abuse policy, including having a positive drug-test result, may lead to disciplinary action, up to and including dismissal.

The proper use of medication prescribed by your physician is not prohibited; however, we do prohibit the misuse of prescribed medication. Employees' drug use may affect their job performance, such as by causing dizziness or drowsiness. It is the employee's responsibility to determine from his/her physician whether a prescribed drug may impair safe job performance and to notify a supervisor of any job restrictions that should be observed as a result.

## ALCOHOL & ALCOHOL ABUSE

The consumption of alcohol while on Company premises is **prohibited without approval from a Department VP and the Human Resources Department**. Consumption of alcohol can constitute serious violations of Company rules, jeopardize the Company and can create situations that are unsafe or that substantially interfere with job performance. Under certain circumstances alcohol may be consumed at company group functions, by employees of legal age, with VP and H.R. approval, however, employees are expected to conduct themselves properly in a safe and professional business manner at all times. Employees in violation of the policy are subject to appropriate disciplinary action, up to and including discharge. Additionally, Telenav reserves the right to require an employee to undergo a medical evaluation or blood alcohol test under appropriate circumstances.

Any employee suspected of consuming alcohol without prior VP approval is subject to reasonable inspection and search, with or without notice. Employee's personal belongings, including any bags, purses, briefcases and clothing and all Company property, are also subject to reasonable inspection and search, with or without notice. Employees who violate the Company's Alcohol Abuse policy will be removed from the workplace immediately. The Company may bring the matter to

the attention of appropriate law enforcement authorities. Any conviction for criminal conduct involving alcohol whether on or off duty, or any violation of the Company's alcohol abuse policy may lead to disciplinary action, up to and including dismissal.

## ACCOMMODATION AND REHABILITATION OF CHEMICAL DEPENDENCIES

The Company will attempt to reasonably accommodate an employee with chemical dependencies (alcohol or drugs), if he/she voluntarily wishes to seek treatment and/or rehabilitation. An employee desiring such assistance should request an unpaid treatment or rehabilitation leave of absence. The Company's support for treatment and rehabilitation does not obligate the Company to employ any person who violates the Company's foregoing drug and alcohol abuse policy or whose job performance is impaired because of substance abuse. Additionally, the Company is not obligated to reemploy any person who has participated in treatment or rehabilitation if that person's job performance remains impaired as a result of a dependency. Employees who are given the opportunity to seek treatment and/or rehabilitation and are involved in any further violations of this policy will not be given a second opportunity to seek treatment or rehabilitation.

## APPEARANCE, CONDUCT & LANGUAGE

Telenav expects employees to maintain a neat, well-groomed, professional appearance at all times, which includes the language and tone in which they communicate.

Telenav is a business casual working environment. Employees are expected to dress in an appropriate professional manner during working hours, at company sponsored events, and at any time an employee is representing Telenav.

The Company requires order and discipline to succeed and to promote efficiency, productivity, and cooperation among its employees. The orderly and efficient operations of Telenav require that employees maintain proper standards of conduct at all times.

Employees who fail to maintain proper standards of conduct toward their work, their co-workers or the Company's customers, or who violate any of the Company's policies, are subject to appropriate disciplinary action, up to and including discharge.

All instances of misconduct should be referred to the Human Resources Department immediately.

## ANTI-NEPOTISM POLICY

Members of an employee's immediate family will be considered for employment based on their qualifications. Immediate family may not be hired, however, if employment would:

- (i) create a supervisor/subordinate relationship with a family member;
- (ii) Have the potential for creating an adverse impact on work performance; or

(iii) Create either an actual conflict of interest or the appearance of a conflict of interest.

This policy must also be considered when assigning, transferring, or promoting an employee. For the purpose of this policy, immediate family includes: spouse, parent, child, sibling, in-law, aunt, uncle, niece, grandparent, grandchild, members of household. This policy also applies to romantic relationships.

Employees, who become immediate family members or establish a romantic or unusually close personal relationship, may continue employment as long as it does not involve any of the above. If one of the conditions outlined should occur, attempts will be made to find a suitable position within Telenav to which one of the employees will transfer. If employees become immediate family members or establish a romantic relationship, the Company will make reasonable efforts to assign job duties to minimize problems of supervision, safety, security or morale. If accommodations of this nature are not feasible, the employees will be permitted to determine which of them will resign. If the employees cannot decide, the Company will decide in its sole discretion who will remain employed.

### **ROMANTIC OR SEXUAL RELATIONSHIPS**

Consenting "romantic" or sexual relationships between a supervisor/ manager and an employee may at some point lead to unhappy complications and significant difficulties for all concerned - the employee, the supervisor/manager and the Company. Any such relationship may, therefore, be contrary to the best interests of the Company.

If a romantic or sexual relationship between a supervisor/manager and an employee should develop, it shall be the responsibility and mandatory obligation of the supervisor/manager promptly to disclose the existence of the relationship to the employee's Department Head. The employee may make the disclosure as well, but the burden of doing so shall be upon the supervisor/manager.

The company recognizes the ambiguity of and the variety of meanings that can be given to the term "romantic". It is assumed, or at least hoped, however, that either or both parties to such a relationship will appreciate the meaning of the term as it applies to either or both of them and will act in a manner consistent with this policy. Sexual relationships shall be considered a romantic relationship, which shall require disclosure in accordance with this policy.

The Department Head shall inform others with a need-to-know of the existence of the relationship, including in all cases the person responsible for the employee's work assignments.

This policy shall apply without regard to gender and without regard to the sexual orientation of the participants in a relationship of the kind described.

### **INJURY AND ILLNESS PREVENTION PROGRAM**

The health and safety of employees and others on Company property are of critical concern to the Company. We strive to attain the highest possible level of safety in all activities and operations. The

Company also intends to comply with all health and safety laws applicable to our business.

To this end, the Company must rely upon employees to help keep work areas safe and free of hazardous conditions. Employees should be conscientious about workplace safety, including proper operating methods and known dangerous conditions or hazards. You should report any unsafe conditions or potential hazards to your supervisor *immediately*, even if you believe you have corrected the problem. If you suspect a concealed danger is present on the Company's premises, or in a product, facility, piece of equipment, process, or business practice for which the Company is responsible, bring it to the attention of your supervisor *immediately*.

Additionally, the Company has developed a written Injury and Illness Prevention Program as required by law. A copy of the Program is available for your review from the Human Resources Department. In addition to attending any training required by the Company, it is your responsibility to read, understand and observe the Injury and Illness Prevention Program provisions applicable to your job.

### **VIOLENCE IN THE WORKPLACE**

The Company strongly believes that all employees should be treated with dignity and respect. Acts of violence will not be tolerated. Any instances of violence must be reported to the employee's supervisor and/or the Human Resources Department. All complaints will be fully investigated.

The Company will promptly respond to any incident or suggestion of violence. Violation of this policy will result in disciplinary action, up to and including immediate discharge.

### **ACCIDENTS & EMERGENCIES**

Maintaining a safe work environment requires the continuous cooperation of all employees. The Company strongly encourages employees to communicate with fellow employees and their supervisor regarding safety issues.

All employees will be provided care, first-aid and emergency service, as required, for injuries or illnesses while on Telenav premises. Employees should contact their supervisor, the nearest supervisor, and/or 911 in the event of an accident or emergency.

If an employee is injured on the job, Telenav provides coverage and protection in accordance with the Worker's Compensation Law. When an injury is sustained while at work, regardless of the severity of the injury or accident, it must be reported immediately to the employee's supervisor, who in turn will notify Human Resources of the incident. *If medical attention is required immediately, supervisors will assist employees in obtaining medical care, after which the details of the injury or accident must be reported.*

### **WORKERS' COMPENSATION INSURANCE**

Should a work-related injury or illness occur, Workers' Compensation Insurance may provide for the payment of medical expenses as well as partial salary continuation.

You must immediately report a work-related injury or illness to your manager and Human Resources, regardless of the severity of the injury or accident. Human Resources will inform the Workers' Compensation carrier of your injury or illness and will work with you to ensure receipt of all applicable benefits, i.e., Workers' Compensation insurance (covering payment for medical treatment and lost wages), vacation pay, etc. Benefits claims, in conjunction with work-related injury or illness, may be jeopardized by failure to report them in a timely manner.

Failure to report accidents is a serious matter as it may preclude an employee's coverage under Worker's Compensation Insurance.

### **ACTIVITIES NOT COVERED**

From time to time, you may be asked to sign a waiver stating that you understand that injuries incurred during voluntary (i.e., not required) extracurricular activities will not be covered by Workers' Compensation Insurance. In seeking treatment for such an injury, please be sure to follow normal procedures as prescribed by your plan choice just as you would for any other non-work related injuries or illnesses.

### **SMOKING POLICY**

To comply with government regulations, Telenav has prohibited smoking throughout its workplace, including inside all enclosed buildings, except in designated smoking areas. *Employees wishing to smoke must do so at least 20 feet away from all entrances and windows that open and smoking must occur during scheduled work breaks.* The employee's direct supervisor should approve all smoke breaks.

Employees who observe other individuals smoking in the workplace have a right to object and should report the violation to their supervisor or another member of management. No employee will be disciplined or retaliated against for reporting smoking that violates California law or Company policy. Any violation of this policy may result in appropriate corrective disciplinary action, up to and including discharge.

Any questions regarding the smoking policy should be directed to the Human Resources Department.

### **OPEN DOOR POLICY**

Telenav promotes an atmosphere whereby employees can talk freely with members of management. Employees are encouraged to openly discuss with their supervisor any problems so appropriate action may be taken. If the supervisor cannot be of assistance, Human Resources are available for consultation and guidance. Telenav desires to provide an environment that supports success and happiness for all our employees. We, therefore, welcome the opportunity to help employees whenever feasible.

### **INTERNAL COMPLAINT PROCEDURES**

To foster sound employee-employer relations through communication and reconciliation of work-related problems, Telenav provides employees with an established procedure for expressing employment related concerns.

In situations where employees feel a complaint is in order, the following steps should be taken:

If an employee believes that he/she has a legitimate work-related complaint, the employee is encouraged to first attempt to resolve the issue(s) through discussions with his/her immediate supervisor.

If the situation is not resolved after the complaint is discussed with the employee's immediate supervisor, or if the complaint involves the employee's immediate supervisor or the employee does not feel comfortable going to his or her direct supervisor with the issue, it should be brought to the attention of the next level supervisor or a representative in the Human Resources Department with written documentation. The Company will attempt to resolve the complaint within a reasonable period while preserving the confidentiality and privacy of those involved to the extent feasible.

### **FRAUD / DISHONESTY / ETHICS**

Telenav considers any act of fraud or dishonesty on the part of its employees as unacceptable conduct, and it will not be tolerated. Acts that are considered to be either fraudulent or dishonest include, but are not limited to the following:

1. Theft of any kind, including cash, expense or salary abuse.
2. Any effort to mislead, manipulate or engage in fraudulent influence of any Telenav accountant or independent accountant or auditor.
3. The making of false or misleading entries in any of the Company's books, records or financial documents, including any materials prepared for or submitted to any Telenav accountant or independent accountant or auditor.
4. The alteration, destruction, mutilation, concealment, covering up or falsification of any Telenav book, record or file or any entry in any book, record or file.
5. The making of any threat, request or suggestion that any employee engage in any of the types of the fraudulent or dishonest activity listed in this policy

Any employee who is aware of any example of any of the above types of conduct occurring or having occurred, or who suspects that such conduct may be occurring, should report their suspicions to their Manager, any Manager, or the Company's Corporate Compliance Officer. Refer to the Company Whistleblower Policy for instructions on how to raise a compliance concern or retaliation complaint.

Nothing in this or any other Telenav policy or any other agreement between an employee and Telenav shall limit, prohibit or restrict any employee from engaging in any Protected Activity as defined by the Company Whistleblower Policy.

Retaliation against any employee because of his or her bringing forward, in good faith, any questions, concerns or complaints about any of the above types of behavior, including concerns about accounting or auditing matters, recording of information, record retention or in any other way concerning the honesty and integrity of the Company's operations, is strictly prohibited. Telenav also prohibits retaliation against any employee who provides accurate information to any law enforcement or regulatory body about the actual or possible commission of any federal offense. Any employee who believes, in good faith that he or she has been retaliated against or threatened with retaliation for these reasons should report the matter immediately to the Human Resources Department or, if it concerns questionable accounting or auditing matters, to the General Counsel and/or Audit Committee.

If complaints about any of the types of conduct described in this policy are made, Telenav will promptly undertake to investigate the complaint and will do so thoroughly and effectively. All employees who are asked to participate in the investigation are expected to do so and to provide complete and honest information and documents in a timely manner. Failure to do so may subject the employee to disciplinary action, which may include discharge.

If as a result of the investigation, Telenav determines that an employee was aware of the dishonest or fraudulent conduct and did not report it as required, that employee is subject to disciplinary action, which may include discharge.

## **SOLICITATIONS, DISTRIBUTIONS AND USE OF BULLETIN BOARDS**

Employees may not solicit any other employee during working time, nor may employees distribute literature in work areas at any time during working time. Under no circumstances may an employee disturb the work of others to solicit or distribute literature to them during their working time.

Persons not employed by Telenav may not solicit or distribute literature or other materials to Telenav employees for any purposes on Company premises.

### **Bulletin Boards**

Bulletin boards maintained by Telenav are to be used only for posting or distributing material of the following nature:

Notices containing matters directly concerning Company business; and HR approved postings.

Announcements of a business nature which are equally applicable and of interest to employees.

All posted material must have authorization from Human Resources. All employees are expected to check these bulletin boards periodically for new and/or updated information and to follow the rules set forth in all posted notices. Employees are not to remove material from the bulletin boards.

## **INTERNAL INVESTIGATION & SEARCHES**

From time to time, Telenav may conduct internal investigations pertaining to security, auditing or work-related matters. Employees are required to cooperate fully with and assist in these investigations if requested to do so.

Whenever necessary, in the Company's discretion, work areas (i.e., desks, file cabinets, etc.) and personal belongings (i.e., brief cases, handbags, etc.) may be subject to a reasonable search without notice. Employees are required to cooperate.

The Company will generally try to obtain an employee's consent before conducting a search of work areas or personal belongings, but may not always be able to do so.

## **REFERENCE CHECKS**

All inquiries regarding a current or former Telenav employee must be referred to the Human Resources Department.

Should an employee receive a written request for a reference, he/she should refer the request to the Human Resources Department for handling. No Telenav employee may issue a reference letter or verbal reference to any current or former employee without the permission of the Human Resources Department.

Under no circumstances should any Telenav employee release any information about any current or former Telenav employee over the telephone. All telephone inquiries regarding any current or former employee of Telenav must be referred to the Human Resources Department.

In response to an outside request for information regarding a current or former Telenav employee, the Human Resources Department will furnish or verify only an employee's name, dates of employment, job title and department. No other data or information regarding any current or former Telenav employee, or his/her employment with Telenav, will be furnished unless the employee authorizes Telenav to furnish this information in a writing that also releases Telenav from liability in connection with the furnishing of this information or Telenav is required by law to furnish any information.

## **EMERGENCY CLOSING POLICY**

At times, emergencies (such as severe weather, fires, power failures, earthquakes, etc.) can disrupt company operations. In extreme cases, these circumstances may require the office to be closed. If such an emergency occurs, HR will send out a corporate email as to whether Telenav has decided to close the office or not.

Employees may use available vacation time during adverse weather conditions when Telenav has not declared an emergency closing.

When the office is officially closed due to emergency conditions, the Company will pay the time off from scheduled work.

In cases where an emergency closing is not declared, employees must use accrued vacation time for any absence.

## **MOBILE DEVICES**

### **MOBILE DEVICE EXPENSE REIMBURSEMENT**

- Business Use
- Mobile devices for business use may be provided to authorized employees at the level of Manager (with direct reports) and above, along with certain other professionals, including:
  - those who are on call 24/7;
  - individuals traveling outside of the company's offices or outside sales team members; or
  - employees who travel frequently on company business.

The Company will support cell phone use by authorized employees via two options available:

(1) enrollment in the Company's corporate cell phone plan where a device and plan are provided at the Company's choosing. Such employee should work with the IT department to transfer to the corporate plan centralized billing. The IT department will evaluate appropriate plans, features, i.e., minutes, data plans, etc., to ensure the appropriate service arrangement.

#### **OR**

(2) reimbursement to employees of \$100 a calendar quarter (and proration therein) for usage via an employee's own personal device ONLY if such device is enabled such that it is capable of receiving Company emails. Under this selected option, the Company will NOT reimburse for the cost of a device purchase or rental at any time. Reimbursement will be made upon submission of an expense report on a quarterly basis no later than 30 days after each calendar quarter. The Company will reimburse for greater usage upon submission of documentation establishing the business use of the device exceeds the \$100 reimbursement amount.

The Company will not support employee's election of both available options. All additional needs for company provided cell phones will require the prior approval of the Director of Human Resources. Company provided cell phones should include basic plan services, including appropriate voice and data plans. Telenav premium service will be provided on all authorized company provided cell phones only. For Company provided phones, the cell phone service provider assigned to an employee will be determined at the sole discretion of the Company.

The Company will support the porting to and from of a personal phone number for use by the employee while an employee at Telenav.

For Company issued phones, employees at no time and for no reason should remove the SIM card from their Telenav issued business device and place in any other phone, except for those employees in the Engineering organization who are performing engineering development, porting, testing, and QA work. If such SIMs are removed, notification must be

provided to IT which is tracking phone plans by device and phone number. Temporary removal of a SIM with a local SIM (ie; when traveling in China) is appropriate under certain circumstances to save money on long distance voice and data needs.

Employees requesting more than one cell phone service must obtain prior approval from the Company's CFO.

When traveling internationally on business, employees are requested to utilize their cell phone rather than a hotel phone. Loaner cell phones are available in the IT department for short-term use when traveling on business internationally. IT must be notified at least 2 weeks prior to traveling internationally to ensure that the respective phone is set up for international use. When traveling internationally on personal business, international service will only be provided for Director level and above to allow them to "stay connected." Any international charges billed to an employee's Telenav issued number while traveling for personal reasons will be the financial responsibility of the employee and will not be reimbursed.

Employee purchases of cell phones, PDAs, and other mobile devices will NOT be reimbursed unless authorized in advance by the Company and upon establishing that the device is required for the employee's job. All such purchases must be procured through the IT department and ONLY if you have elected to be on a Company provided plan. Replacement of damaged and lost cell phones will be facilitated on a case by case basis. If an employee has multiple issues with damaging or losing Company issued phones, the Company, at its discretion, may choose to no longer issue the employee a Company phone. The Company will endeavor to recycle phones previously utilized elsewhere in the organization (i.e.; testing and development, etc.) where feasible.

Employees may not purchase any applications on their Telenav issued device without approval from the Director of Human Resources.

The Company's policy will allow replacement of devices no sooner than every 24 months for personal business use. Any exceptions require the prior approval of the Company's CFO. Employees must return old devices immediately upon receiving their new device.

All Telenav employees will be required to turn in their Company issued device upon termination or last day of employment along with all accessories and SIM card.

Any lost or stolen devices should be reported to IT and HR IMMEDIATELY.

As a courtesy to callers and to assist us in managing our cell phone records, the Company requires that all phones must have voicemail activated with the requisite employee's name (otherwise they are subject to inactivation).

Also, to more effectively manage costs, any company provided cell phones with zero voice and data usage for 90 days or more will be subject to being inactivated.

Other Purposes (Demo, Testing and Development)

The Company's IT dept. will facilitate the ordering, distribution, and recycling of phones to be used for demonstration, testing, and development. All such requests should be processed through the Footprints equipment request approval process. Such devices and service distributed will be treated as "on loan" to the designee. Any requests made for non-employee users will be handled on a case by case basis depending on the underlying circumstances and business need. Retrieval of these devices for non-employee users will be the responsibility of the person requesting the device.

The Company's IT dept. will track the status of all "loaned out" phones for demo, testing, and development purposes and will seek return of all devices and related SIMS.

## **MOBILE DEVICE HANDS-FREE POLICY**

Employees should review the most current version of the Company's Mobile Device Hands-Free Policy.

## **MOBILE DEVICE PHYSICAL ASSET SECURITY**

Users should take precautions to protect mobile computing equipment:

- Users are responsible for the physical security and care of end user computing equipment.
- Users must employ reasonable means to physically secure their computing equipment when not in use, including using locking devices or storing in a locked cabinet to minimize the risk of loss or damage to a laptop.
- Users must lock devices in a secure compartment when left unattended. Devices left unattended in vehicles must not be visible.

## **TRAVEL SECURITY PRECAUTIONS FOR MOBILE DEVICES**

Users are expected to take precautions to protect assets and data while traveling. Users are required to:

- Not access information that is classified as confidential in a public place, such as on a train, aircraft, bus, or on any unsecured wireless connection, such as a coffee shop if it can be viewed by others.
- Not leave an asset containing information unattended in unsecured public areas, such as airport lounges, check-in counters, hotel lobbies, restrooms and conference centers.
- Not put computing equipment in checked baggage when traveling, except as required by law.
- Only place computing equipment on X-Ray or other security scanning systems to coincide with their entering the human scanning systems to minimize the opportunity of theft.
- Users should label computing equipment and carrying cases with their desk or mobile telephone number and must not use a business card or any other identifier with the

logo of Telenav partners or Telenav customers.

- Store computing equipment in a hotel room safe where available.
- If a suitable room safe is not available, then users should keep the computing equipment in the user's possession whenever reasonably possible.
- If a room safe is not available and if it is unreasonable to keep the computing equipment in the user's possession, user may leave the device(s) in the hotel room, however, the user must make all reasonable efforts to secure or hide the device(s) within the locked hotel room.

## **MOBILE DEVICE ACCEPTABLE USE**

All users that access email or corporate data using mobile devices are expected to:

- Only load data essential to their role onto their mobile device(s).
- Ensure that devices are not "jailbroken" or have any software/firmware installed that is designed to gain access to functionality not intended to be exposed to the user.
- Not load pirated software or illegal content onto their devices.
- Users must not use corporate workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

## **TELENAV ISSUED DEVICES**

Telenav issued mobile devices may:

- Not connect devices to any non-Telenav assigned computer/workstation.
- Not be shared with anyone not authorized by the primary user to operate the device

## **EMPLOYEE-OWNED (BYOD) DEVICES**

All users that would like to connect personal Bring Your Own Device (BYOD) to connect to Telenav data must:

- Receive prior approval from their manager and IT Director
- Applications must only be installed from official platform-owner approved sources.
- Upon termination of employment, Telenav will remove any Telenav-related data through a remote process.

## **TECHNICAL REQUIREMENTS**

### **MOBILE DEVICE CONFIGURATION**

Mobile devices must be configured:

- Devices must use the following Operating Systems: Android 4.4 or later, IOS 9.x or later.
- All portable computing devices must be encrypted with a full device encryption solution.
- To lock the screen after 15 minutes of inactivity.

## MOBILE PASSWORD REQUIREMENTS

Mobile devices must be configured:

- At a minimum, with a secure passcode or two-factor authentication. This passcode must not be the same as any other credentials used within the organization.
- To store all user-saved passwords in an encrypted password store.
- Utilize a password that consists of at least 5 characters.

## MOBILE DEVICE UPDATES

Devices must be kept up to date with manufacturer or network provided patches. At a minimum, patches should be checked for weekly and applied at least once a month

## REMOTE WIPE CAPABILITY

All mobile devices should be configured with the ability to remotely wipe all corporate data. Users that access corporate data agree to this capability being enabled on their personal mobile devices as well. Device may be wiped:

- If the device is lost or stolen
- After 10 failed sign-on attempts
- If a corporate-owned device has not been returned

## USE OF COMPANY EQUIPMENT

The Company provides any supplies, equipment, and materials necessary for you to perform your job. These items are to be used solely for the Company's purposes. Employees are expected to exercise care in the use of Company equipment and property and use such property only for authorized purposes. Loss, damages or theft of Company property should be reported at once. Negligence in the care and use of Company property may be considered grounds for discipline, up to and including discharge.

The Company's equipment, such as telephone, postage, facsimile and copier machine, is to be used for business purposes. An employee may only use this equipment for non-business purposes in an emergency and only with the permission of his or her supervisor. Personal usage, in an emergency, of these or other equipment that results in a charge to the Company should be reported immediately to your supervisor or accounting so that reimbursement can be made.

Upon discharge of employment, the employee must return all Company property, equipment, work

product and documents in his or her possession or control.

## TELEPHONE USE

Because a large percentage of our business is conducted over the phone, it is essential to project a professional telephone manner at all times.

Although Telenav realizes that there are times when an employee may need to use the telephone for personal reasons, it is expected that good judgment will be used in limiting the length and frequency of such calls. Additionally, no long distance personal calls may be made on Company phones without prior approval from the employee's supervisor.

## NOTICE TO CSRs

Telephone conversations with subscribers and others who call Customer Service Representatives (CSRs) on the incoming business lines will be monitored and/or recorded from time to time for CSR training, quality control, and other business purposes. This notice provides information to employees about monitoring and recording practices.

So that callers may be aware of the possibility of all monitoring and/or recording, all monitoring (other than by traditional, unmuffled "open mike" extensions) is preceded by a pre-recorded (or live) announcement over the phone to each caller, stating that "to assure service quality, calls are sometimes monitored and/or recorded."

It is Company policy not to monitor or record any personal or confidential calls, except to the extent of determining the personal or confidential nature of such calls. The following practices are used to promote the privacy of all personal and confidential calls:

- (1) The telephones on which CSR's receive calls on the outside line are not to be used for personal calls by CSR's or other company employees, because those phones are subject to monitoring. Other phones are available in the office to be used for any necessary personal calls.
- (2) Telephones that may be monitored are customarily labeled or marked: "To assure service quality, calls are monitored."
- (3) Supervisors who conduct service monitoring should simply leave the line immediately if they monitor a call which for any reason seems to be personal or confidential in nature.

## PHOTOGRAPHY AND RECORDING RESTRICTIONS

- Mobile devices equipped with camera / video capabilities are permitted unless local facility policy prohibits their use.
- Local facility management has the right to restrict or forbid the making of images or videos with mobile devices equipped with camera and / or video capabilities.
- Permission must be obtained from your supervisor or project lead before taking photos,

recording sound or video of any confidential information.

- Written permission must be obtained from individuals or management involved before publishing or sending photos, recorded sound or video to anyone else or to any website.

## **AUDIO RECORDING POLICY**

It is a violation of Telenav policy to record conversations unless prior approval is received from your supervisor or a member of upper-level management **and** all parties to the conversation give their consent. It also is illegal under California law to record a conversation without every party to the conversation consenting to the recording.

The purpose of this policy is to eliminate a chilling effect on the expression of views that may exist when one person is concerned that his or her conversation with another is being secretly recorded. This concern can inhibit spontaneous and honest dialogue especially when sensitive or confidential matters are being discussed.

## **PHYSICAL SECURITY**

Telenav will utilize access controls to restrict access to the minimum number of authorized personnel required and prevent unauthorized access to the building and secured areas.

To provide a safe and secure workplace, commercially reasonable monitoring of the building and computer room are in place twenty-four (24) hours a day, seven (7) days a week.

## **PHOTO ID/ACCESS BADGES**

### **A) EMPLOYEES**

All Telenav employees are issued a Photo ID/Access Badge upon hire to enter the buildings. Everyone is required to wear their Photo ID/Access Badge in plain view while on Telenav property. Employees may choose whether to wear their badge on a lanyard around their neck or on a pulley attached to their belt/waist.

All entrance doors are set to automatically lock upon closing for safety and the security of our employees and property. Under NO circumstances should any door be propped open for any reason. While the Photo ID/Access Badges allows access to the doors for entry into the building, certain individuals may have access restrictions including specific hours or access and/or restricted access to certain rooms within the building itself. Every badge is electronically assigned to an individual allowing us to track who and when someone has entered the building or a secured area at a given time. This tracking is for the individual's safety as well as the security of our property. It is extremely important for everyone to understand the importance of security. No Telenav employee should ever allow anyone to "Tail Gate" (allow any other person, be it another employee, delivery person, guest, etc. to follow them in the building or secure area after swiping their badge.) If someone claims to work at Telenav or you think they may look familiar but he/she does not

have a Photo ID/Access Badge with them, you should direct them, to the front lobby where they can sign in and be given a temporary badge.

Under no circumstances should any Telenav employee allow anyone without a Photo ID/Access badge into any door other than the front lobby door in the building. Anyone trying to gain access into the building that does not have a Photo ID/Access badge should be directed to the reception area/front entrance where they can be signed in, this includes people you may recognize as an employee. This policy is for the safety of all employees and the security of our property.

If your badge is lost or stolen, you must obtain a replacement. Lost or stolen badges should be reported to your manager and the Facilities Team, as soon as possible. Failure to wear your Photo ID/Access badge or causing excessive loss or damage to badges can lead to disciplinary action.

Employees should stop anyone they see walking around the building without a badge and offer assistance. Anyone without a badge should be escorted to the front desk where they can obtain a replacement badge or a visitor badge.

Upon leaving the company, employees will be required to return ID badges to their Manager or Human Resources as part of the Exit Process.

### **B) CONTRACTORS/CONSULTANTS, INTERNS AND TEMPORARY EMPLOYEES**

Contractors/Consultants, Interns, and Temporary Employees with assignments of two or more weeks will be issued a photo ID badge. Those with a shorter assignment will be issued a Telenav ID badge without a photo. The ID badge must be worn on a lanyard around the neck or on a pulley attached to their belt/waist at all times. Access to additional secured areas will be addressed on a case by case basis.

Contractors/Consultants, Interns, and Temporary Employees are required to return ID badges to their Manager or Human Resources on the last day of their assignment.

### **C) VISITORS**

All visitors must sign in with the front desk before entering the main building. All visitors will be issued a Visitor/Guest badge identifying them as a visitor/guest. Visitor/Guest badges have a large "V" where a picture would be and is worn with a red lanyard that has "visitor" written on it. A Telenav employee must accompany all visitors/guests at all times. The receptionist will notify the Telenav employee that their visitor/guest is in the lobby. It is then the Telenav employee's responsibility to come get their visitor/guest and escort them throughout their visit at Telenav. A Telenav employee should escort all visitors/guests back to the main lobby at the end of their visit to sign out and return their badge.

Access logs for visitors will be retained to demonstrate when visitors signed in/out and who they were visiting.

## AUTHORIZED ACCESS ONLY

Telenav considers the Data Center as extremely sensitive and access is only granted to authorized personnel and support staff.

## PRODUCTION SERVICES

Production Services are located in remote data centers or cloud platforms that include monitoring of:

- Physical intrusion, unlawful and unauthorized physical access
- Heating, ventilation or air conditioning problems
- Power failures or outages (i.e., Uninterrupted Power Service)
- Fire
- Theft
- Natural disasters (reasonable protection)

## PORT ACCESS SECURITY

By default, all unused network, hardware diagnostic, configuration and management ports will be disabled. Proper authorization from the system owner is required before access can be provided.

## PROTECT SENSITIVE INFORMATION

Telenav users are often entrusted with sensitive information. It is the responsibility of the user to read the Telenav *Data Classification Policy*, and understand what data is considered sensitive and how to properly handle it. Some of the requirements include:

- Protecting sensitive information from casual observation or theft, (e.g., don't leave sensitive information unattended).
- Limiting access to information, including paper hard copies, only to persons or systems authorized by under written agreement
- Restricting access to any Personally Identifiable Information to authorized individuals
- Maintaining a backup of their critical files.
- The disposal and/or destruction of Telenav information by following the appropriate company policy for information retention, data classification and handling controls.

## STORING DATA ON LAPTOPS

Laptop users should make all reasonable efforts to:

- Store Telenav Information on a secured server, where access is controlled, (e.g., 'H' drive, network 'S' drive, SharePoint).
- Not store Telenav Information on a laptop for any longer than is necessary to fulfill a specific business need and delete or transfer laptop data to a secure device as soon as practically possible.

## ACCOUNTABILITY

Use of Telenav information resources and assets is based on the principle of individual accountability and segregation of duties. Each individual user is personally responsible for all activities, whether intentional or unintentional conducted under his/hers user identification code(s) or assigned information assets.

## REPORTING INCIDENTS

Users are expected to report any suspected unauthorized access to company data.

Telenav users should report any suspected incidents or policy violations to the Telenav help desk or Information Security department immediately. Incidents can include, but are not limited to:

- The theft or loss of Telenav owned system or any system with Telenav data on it
- The intentional or unintentional disclosure of Telenav data
- Vulnerabilities in Telenav systems, applications, or networks
- Malware or virus infections

## LOST OR STOLEN DEVICE

If a laptop, cell phone, tablet, or other mobile device is lost or stolen, the user must immediately notify their management, the service desk, and IT Information Security.

- For Telenav-issued cellular devices, open a case with the service desk and request the service be stopped
- For employee/user owned cellular devices, contact the appropriate wireless carrier or vendor and request account/device suspension

## IT SYSTEMS POLICY

Every Telenav employee is responsible for using the IT Systems, properly and in accordance with this policy.

All users are responsible for protecting and maintaining the confidentiality, integrity and availability of Telenav information resources. Telenav employees, contractors, interns, hereinafter referred to as "Users", are granted access to Telenav IT systems for the limited and express purpose of executing their job responsibilities.

Users are reminded of their responsibility to protect Telenav information from unauthorized disclosure or loss, and to conduct themselves in a moral, ethical and lawful manner. This policy is designed to help Users understand Telenav expectations for the use of these information resources and assets.

This policy is designed to protect Telenav, our employees, customers and other partners from harm

caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions. Unauthorized or inappropriate use of electronic communications systems can cause, among other things:

- network and systems downtime
- virus or malware infections
- potential legal and financial penalties for data leakage

The IT System is the property of Telenav. It has been provided by Telenav for use in conducting company business. All communications and information transmitted by, received from, or stored in this system are company records and the property of Telenav. The IT System is to be used for company purposes only. Use of the Email system for personal purposes should be limited. Personal emails will become the property of Telenav if accessed through Telenav's servers.

Employees should have no expectation of privacy (other than provided by local laws) in any matter stored in, created, received, or sent over the Telenav IT System.

Telenav, in its discretion as owner of the IT System, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the IT System, for any reason and without the permission of any employee.

Even if employees use a password to access the IT System, the confidentiality of any message stored in, created, received, or sent from the Telenav IT System still cannot be assured. Use of passwords or other security measures does not in any way diminish Telenav's rights to access materials on its system, or create any privacy rights of employees in the messages and files on the system. Any password used by employees must be revealed to Telenav as email files may need to be accessed by the Company in an employee's absence.

Employees should be aware that deletion of any email messages or files will not truly eliminate the messages from the system. All email messages are stored on a central back-up system in the normal course of data management.

Even though Telenav has the right to retrieve and read any messages (whether oral or written) or files transmitted on the Telenav IT System, those messages and files should still be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any messages or files that are not sent to them. Any exception to this policy must receive the prior approval of Telenav management.

Telenav's policies against sexual or other harassment apply fully to the IT System, and any violation of those policies is grounds for discipline up to and including discharge. Therefore, no messages or files should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, physical or mental disability, legally protected medical condition, genetic information, ancestry, citizenship status, marital status, family care status,

creed, gender, veteran status, sexual orientation or any other classification protected by law.

The IT System may not be used for solicitation of any name, regardless of whether such solicitation is for charitable, religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations. Telenav will not discipline employees for conduct protected by National Labor Relations Act and other comparable federal, state and local laws.

The IT Systems shall not be used to send (upload) or receive (download) unlicensed copyrighted materials, or similar materials without prior authorization from Telenav management. The IT Systems should not be used to send trade secrets or proprietary financial information to non-Telenav resources without authorization from your supervisor. Employees, if uncertain about whether certain information is appropriate for transfer, should resolve all doubts in favor of not transferring the information and consult with Telenav management.

Without the express permission of their supervisors, employees may not send unsolicited email to persons with whom they do not have a prior relationship.

Management approval is required before anyone can post any information on commercial on-line systems or the Internet; provided, however employees may post information on the Internet in conjunction with the Company's social media marketing efforts subject to Telenav's Social Media Policies. Any approved material that is posted should obtain all proper copyright and trademark notices. Absent prior approval from Telenav to act as an official representative of Telenav, employees posting information must include a disclaimer in that information stating, "Views expressed by the author do not necessarily represent those of Telenav."

Also refer to the separate Telenav Record Retention Policy on the intranet.

Employees are reminded to be courteous to other users of the IT System and always to conduct themselves in a professional manner. emails and/or voice mails are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. Users should write email communications and/or record voice mails with no less care, judgment and responsibility than they would use for letters or internal memoranda written on Telenav letterhead.

Employees should also use professional and courteous greetings on their voice mail boxes so as to properly represent Telenav to outside callers.

Because email records, voice mail records, voice mail messages and computer files may be subject to discovery in litigation, Telenav employees are expected to avoid making statements in email, voice mails or computer files that would not reflect favorably on the employee or Telenav if disclosed in litigation or otherwise.

In order to avoid accidentally disclosing voice mail message contents to unauthorized listeners, employees should not listen to voice mail messages while using the speaker phone feature.

Any employee who discovers misuse of the IT System should immediately contact the Human Resources Department.

Violations of Telenav's IT System and Internet policy may result in disciplinary action up to and including discharge.

## **NO EXPECTATION OF PRIVACY**

The computers and computer accounts given to employees are to assist them in performance of their jobs. The computer system belongs to the Company and may only be used for business purposes.

Except as provided by any applicable national or local law, users shall have no expectation of privacy in anything they create, store, send or receive on Telenav's IT systems, and to the extent permitted by law, users waive all privacy rights in such materials. All email and electronic records are subject to disclosure to enforcement agencies in connection with civil litigation or regulatory investigations.

## **REMOTE ACCESS**

Remote access to the network helps improve productivity, however, it introduces new and serious risks to the infrastructure. The Telenav Remote Access Policy provides guidance for the secure implementation of remote access to the Telenav network.

Remote access will be strictly controlled to protect the confidentiality and integrity of Telenav networks. Telenav will ensure that only approved and secure methods are utilized to access Telenav networks and data.

Only systems owned and provided by Telenav Information Technology department may connect directly to Telenav's internal network.

Remote access to restricted or test internal network segments, systems, or applications may be provided, if the following requirements are met:

- Approval is granted by the requesting departments director-level or above
- Approval is granted by the Information Security department
- Access to production data is strictly prohibited
- The system shall be protected with anti-virus software with current signatures and all relevant software.
- The system is compliant with Telenav's minimum security requirements.

### **REMOTE ACCESS ACCOUNT REQUIREMENTS**

Remote Access Accounts should meet the following requirements:

- Each user will have a unique user ID and password for authentication.
- Shared accounts are not authorized

- Authorization for employee remote access must be approved by a Telenav manager or above and the Information Technology department
- Strong encryption will be utilized in accordance with the *Telenav Information Security Policy*
- Strong passwords will be utilized in accordance with the *Telenav Password Policy*

### **TWO-FACTOR AUTHENTICATION**

Two-factor authentication should be utilized for all remote access to the network by employees, administrators, and third parties. Two-factor authentication may include technologies such as remote authentication, with tokens or VPN with individual certificates.

### **THIRD-PARTY REMOTE ACCESS**

All new requests for vendor or third-party remote access must receive authorization from:

- A Telenav business unit or application owner;
- Director-level signoff for new projects and for new contracting organizations; AND
- Information Security department to provide final sign-off and approval.

All existing requests or renewals for vendor or third-party remote access must receive authorization from:

- Manager-level approval for access by vendors/contractors

Third-Party remote access must be limited to:

- Only those resources that are required to perform job function (specific systems, application, etc.)
- Only the resources requested and approved by Telenav and the Information Security department.

Third-Party Remote Requirements

- Follow Telenav's Information Security Policies, Standards, and Procedures.
- Utilize a unique user ID and password for each user (Credentials may not be shared)
- Assign a management-level single Point of Contact who will be responsible for enforcing Telenav's Information Security Policies, Standards, and Procedures.

### **REMOTE ACCESS IT RESPONSIBILITIES**

The Telenav Information Technology department is responsible for:

- Documenting allowed methods of remote access in Telenav

- Establishing usage restrictions and implementation guidance for each allowed access method
- Enforcing requirements for remote connections
- Monitoring for unauthorized remote access
- Authorizing remote access prior to connection
- Using cryptography to protect the confidentiality and integrity of remote access sessions
- Automatically disconnecting remote access sessions after 30 minutes of inactivity
- Immediately deactivating remote access when it is no longer needed
- All VPN connections must deny network traffic from remote system to un-trusted network (i.e. No split tunneling).

## VPN ACCESS

A VPN, or virtual private network, connection must be used when:

- Connected to a public wired or wireless network. This includes browsing the internet.
- Accessing sensitive information or business-related data

## MULTIPLE NETWORKS CONNECTIONS

Users must ensure that only a single network connection is active when accessing third-party networks and systems (i.e. no additional active connections to wireless networks, home networks)

## WIRELESS ACCEPTABLE USE

Users shall exercise good judgement when using wireless networks, including but not limited to:

- Use caution when connecting to an unknown wifi network such as in a coffee shop or airport. Where possible, users should avoid connecting to open/ non-password protected access points.
- Do not connect personal devices to the Telenav corporate wireless
- Only connect personal (or Non-Telenav issued) devices to the guest wireless network
- Not reveal authentication information for the corporate wireless
- Use approved VPN (Virtual Private Network) when connecting to non-Telenav wireless networks
- Not transmit sensitive or confidential data without a VPN or other Telenav approved connection

## INTERNET USE POLICY

### INTERNET ACCEPTABLE USE

At all times, Users have the responsibility to use company Internet and Intranet communication systems in a professional, ethical and lawful manner. If you abuse your right to use the Internet, it will be taken away from you. In addition, you may be subject to disciplinary action, including possible discharge, and civil and criminal liability. Your use of the Internet is governed by this policy and the IT Systems Policy.

Any access to Telenav's networks, information systems and assets will be conducted over corporately approved, and standards based, connectivity technology. All Internet, business to business and remote user access requires management approval and must include any necessary contractual indemnity controls prior to the access grant.

Employees in the People's Republic of China (PRC) must comply with PRC laws and regulations of internet security (including, but not limited to Article 57 of the PRC Telecommunication Regulations) when using the Internet.

US employees visiting or working in the People's Republic of China (PRC) must comply with PRC laws and regulations of internet security (including, but not limited to Article 57 of the PRC Telecommunication Regulations) when using the Internet.

### DISCLAIMER OF LIABILITY FOR USE OF INTERNET

Telenav is not responsible for material viewed or downloaded by employees from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Employees are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. Employees accessing the Internet do so at their own risk.

### DUTY NOT TO WASTE COMPUTER RESOURCES

Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic. Because audio, video and picture files require significant storage space, files of this or any other sort may not be downloaded unless they are business-related.

## EMAIL AND ELECTRONIC COMMUNICATIONS SYSTEMS ACCEPTABLE USE

Users should exercise good judgment when using email or Internet and Intranet communication systems. Users shall understand that:

- Telenav has the right to monitor, audit, store, retrieve, or otherwise capture any electronic information occurrence, including but not limited to transmissions, sessions, or storage that occurs over its owned, controlled, or connected computing and communication resources, (e.g., email content, Instant Message, Text Messages, voice mail content, network addresses, frequency of occurrence, and identification of specific on-line services).
- Users are not authorized to retrieve any email message unless that user is the intended recipient. Any exception to this policy requires prior approval from Human Resources and only with a legitimate business purpose.
- All Telenav email, instant messaging and social networking messages and associated records remain the sole property of Telenav and may be deleted or disclosed at any time without prior notice.
- Electronic communication systems must not be used to send or receive trade secrets, intellectual property, confidential information, or similar data without prior authorization from the Information Owner, and only using secure methods.
- Telenav provides information on encryption requirements for protecting information being conveyed outside of Telenav as prescribed in Telenav's *Data Classification Policy Standard*.
- Employees should be aware that deletion of any Email messages or files will not truly eliminate the messages from the system. All email messages are stored on a central back-up system in the normal course of data management.
- Physical or electronic files may only be sent, received or used for business in ways consistent with their licenses, copyrights and handling controls as described in the *Data Classification Policy Standard*. Unauthorized peer to peer file-sharing software is not permitted on any Telenav computer.

### E-MAIL RETENTION POLICY

Because email records, IM communications, voicemails, physical and electronics documents and computer files may be subject to discovery in litigation, Telenav employees are expected to save, **(not delete)**, any emails, files or other documents that are subject to any Litigation Holds. Managers must save and not delete **ANY** documents or correspondence pertaining to company policies such as hiring, firing, discipline, etc.

## ACCEPTABLE USE OF SOFTWARE

The following requirements apply to the acceptable use of software. Users shall:

- Only install and use Telenav approved software on Telenav equipment.
- Not install improperly licensed software on corporate systems, including any non-Telenav licensed (privately/user licensed) software or freeware/shareware downloads.
- Have the appropriate license or permission to use the software or other material and are responsible for any consequences of not having the appropriate authorization.
- Not copy software on Licensee computing equipment for installation on home or other computers.
- Obtain the copyright owner's permission before reproducing or photocopying a non-Licensee copyrighted work.

Telenav reserves the right to remove any software not provided by Telenav from its computing equipment without notice to the user.

## REMOVABLE MEDIA ACCEPTABLE USE

Users should ensure due care when using removable media, including but not limited to:

- Avoid storing sensitive information on removable media
- Using only Telenav provided removable media (No personal devices)
- Not plugging in devices that were found or provided by a non-Telenav employee
- Protecting removable media against loss or theft
- Ensuring that Telenav Information stored on removable media is not the sole existing copy
- Reporting lost or stolen removable media containing Telenav data

## SOCIAL MEDIA

Social media networks increasingly serve as effective mass communication channels with respect to both current and potential customers, the media, and other company stakeholders. Engaging in social media networking provides employees with the opportunity to exhibit their sense of community and reflect their individual character and personality via a large-scale media channel.

Postings on social media sites can have a significant effect on how the Company is perceived. We encourage employees to engage in social media, provided that such communications are transparent, ethical, and accurate and you follow the guidelines of

this policy when engaging in social media communications.

The following parameters have been established to provide guidance for employees with respect to participation in any type of social media networking. Employees must always abide by the guidelines when engaging in social media networking. Remember that in an online environment, the lines between public and private, personal and professional are not clear. By identifying yourself as a Telenav, Inc. employee, you are creating a perception about you, your expertise, our shareholders, our customers and the company.

Guidelines outlined in this policy apply when an employee engages such a site during working hours using a company computer and/or during personal time using a personal computer if they represent the company, directly or indirectly at any point by using the company's name or logo.

## **PROFESSIONALISM**

Readers of any posted material may include current or potential clients as well as current or potential employees or other affiliates of Telenav. Therefore, employees are expected to conduct themselves in a respectful, professional manner at all times.

Employees are fully responsible for what they post or otherwise communicate via social media channels. Accordingly, they must always exercise good judgment and common sense.

## **CONFIDENTIAL INFORMATION**

Employees will not post or otherwise communicate any proprietary, confidential and/or insider company information, including but not limited to pricing strategies, rates, product parameters, strategic goals and similar information about Telenav, our affiliates, our partners, our customers, potential customers, or any other entities including employees of Telenav.

Employees will not comment (officially or non-officially) on work-related legal matters or other confidential Telenav matters.

## **CONFLICTS OF INTEREST**

Employees must be clear about their roles, post only information which is correct and within the employees' expertise, and disclose any known or perceived conflicts of interest to management immediately.

## **TRUTHFULNESS**

Employees will only post or otherwise communicate truthful information, using credible sources for credit or validation as needed when quoting, repeating statistics or standards or otherwise representing others' opinions or facts.

## **PERSONAL AND PROPRIETARY INFORMATION**

Employees must always be respectful of any personal and proprietary information of Telenav or of others gained through employment at Telenav, and Telenav's intellectual property and or confidential information. Information sharing practices that govern all Telenav employees under the company's Privacy and Information Security Policies and program parameters apply to all social media communications as well.

## **LEGALITY**

Employees must ensure that all posted information or information otherwise associated with them is presented in accordance with all legal requirements (i.e., copyright laws, fair use laws, proprietary laws, etc.) and meets Telenav high professional standards.

## **POSITIVITY**

Employees will not portray Telenav or any of its customers or employees in a negative or derogatory fashion.

## **SOLICITATION AND MARKETING**

Employees who use Social Media communication for solicitation and/or marketing purposes will need to follow the pre-established review and approval procedure currently in place. Please refer to Marketing and/or Compliance for additional details. This includes use of displaying Telenav's logos.

## **PUBLIC RELATIONS**

Any contacts from the media about Telenav and any of its products, employees, partners, competitors, or otherwise should be referred to the Marketing Department.

## **TELENAV TRADEMARKS**

Employees are prohibited from selling any personal products or services while utilizing Telenav's name or logo, or while on a Telenav branded social media site.

## **SOCIAL MEDIA PRIVACY**

Telenav reserves the right to monitor employees' use of social media channels where Telenav has a branded social media site, including but not limited to a Facebook Fanpage or other Telenav "group" page. However, as detailed above, the employee initiating the communication bears full responsibility and accountability for the content and safety of the information in their communication.

Telenav encourages employees to utilize the Facebook "Permissions" functionality (or similar functionality in other mediums) to block business-related persons, including employees or known customers, from viewing your personal information if you wish to maintain personal privacy.

## **POLICIES APPLY**

Telenav's Code of Business Conduct & Ethics, Standards of Conduct, Non-Disclosure Agreement, Computer Acceptable Use Policy and Anti-Harassment/Anti-Discrimination Policy, Information Security, Data Classification Policy, Secure Customer Data Policy, and other privacy-related policies continue to apply and extend to all forms of communication, including social media (both inside and outside the workplace).

## **ENFORCEMENT**

Telenav will consider a social media site in the same light as any other medium in which something inappropriate information or content is expressed by an employee. Employees are legally liable and may be

sued by an individual or company for anything you write or present online. Employees may be disciplined, up to, and including termination for any commentary or content that are defamatory, proprietary, pornographic, harassing, libelous, that may create a hostile work environment, or that may otherwise violate this policy.

## **CONSENT TO MONITORING**

Telenav (or others acting on Telenav's behalf) maintains the right, to monitor, seize, review, audit, intercept, access, block and disclose all aspects of its electronic systems at any time and without notice or limitation for investigative and quality of service issues. This includes, but is not limited to, email messages and other electronic messages, company provided telephone, Internet site access, chat and newsgroup activity, and downloaded or uploaded material.

## **UNACCEPTABLE USE**

Users are responsible for ensuring email and Internet tools are used in an efficient and ethical manner that complies with this policy and Telenav's corporate policies. Telenav's electronic resources, including email and the Internet, must not be used to access, display, create, transmit, receive or store inappropriate material including, but not limited to, the following:

- Threats
- Pornographic or sexually explicit material
- Material containing derogatory content based on a protected classification, including age, religion, gender, race, national origin, pregnancy, sexual orientation, uniformed service, protected disability status or hate-oriented comments
- Offensive language, or material which is otherwise inappropriate or unlawful
- Discriminatory language or remarks that would constitute harassment of any type
- Junk mail, spam, and chain letters
- Conducting personal business ventures on Telenav information assets

User should also ensure that they do not:

- Knowingly disable or overload any computer system or network, or circumvent any system security intended to protect the privacy or security of another user.
- Engage in tampering with Telenav provided hardware or software including but not limited to anti-virus, VPN, and personal firewall software.
- Engage in unauthorized access, or use, of Telenav information systems through the authorized user's equipment or login.
- Engage in downloading, modification, reverse engineering, de-compiling, disassembly, or the creation of any derivative works of any data or software programs contained in information systems without prior written authorization from Telenav.

- Compromise the malicious code prevention efforts of the company or otherwise create the possibility of malicious code being introduced into Licensee computing systems.

## **BLOCKING OF INAPPROPRIATE CONTENT**

The Company may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by Company networks. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to Company blocking software.

## **PROHIBITED ACTIVITIES**

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, inappropriate, offensive (including offensive material concerning race, color, national origin, religion, creed, sex or gender (including pregnancy, childbirth, or related medical conditions), national origin ancestry, age, physical or mental disability, legally protected medical condition, genetic information, citizenship status, veteran status, marital status, family care status, sexual orientation or other characteristic protected by federal, state or local law), or in violation of Telenav's equal employment opportunity policy and its policies against sexual or other harassment may not be downloaded from the Internet or displayed or stored in Telenav's computers. Employees encountering or receiving this kind of material should immediately report the incident to their supervisors or the Human Resources Department. Telenav's equal employment opportunity policy and its policies against sexual or other harassment apply fully to the use of the Internet and any violation of those policies is grounds for discipline up to and including discharge. Telenav will not discipline employees for conduct protected by National Labor Relations Act and other comparable federal, state and local laws.

## **ILLEGAL COPYING**

Employees may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of your direct supervisor.

## **VIRUS DETECTION**

Files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to email; and files provided by customers or vendors may contain dangerous computer viruses that may damage the Company's computer network. Employees should never download files from the Internet, accept email attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Company-approved virus checking software. If you suspect that a virus has been

introduced into the Company's network, notify the Help Desk immediately.

Violations of this policy will be taken seriously and may result in disciplinary action, including possible discharge, and civil and criminal liability.

Use of the Internet via Telenav's computer system constitutes consent by the employee to all of the terms and conditions of this policy.

## **PASSWORD REQUIREMENTS**

Telenav's system environment is configured consistently to provide the highest levels of security, availability and integrity. This standard provides overall guidance for the consistent application of system and employee passwords in Telenav system environment.

It is understood that not all applications running within Telenav will accept the recommended level of complexity. Users are advised to employ the maximum amount of strong password techniques that can be accepted by the application being used.

Telenav enforces the "strong password" complexity guidelines below. Users are required to adhere to the password control requirements when selecting and using passwords. Passwords must:

- Be at least eight (8) characters long.
- Include at least one (1) uppercase, one (1) lowercase, one (1) number and one (1) special character.
- Password must not contain sequences of three (3) or more characters from the USERID or system name.
- Password must be complex and not contain names, dictionary words, combinations of words, or words with substitutions of numbers for letters.
- Passwords are not to be based on personal information (e.g. names of family, pets, sports teams, hobbies or personal interests, etc.).
- Password must not contain repeating or sequential characters or numbers.
- Passwords should not be based on whole words in any language (including slang, dialect, jargon, etc.).

### **CHANGE DEFAULT PASSWORDS**

Initial default passwords must always be changed, and the new password must meet the password standards outlined. All vendor default passwords must be immediately changed upon installation of the system.

### **ACCOUNT PASSWORD REUSE**

Account passwords will be configured with a history file to remember and prohibit password reuse of the last five (5) passwords.

### **90 DAY EXPIRATION**

All user account passwords are configured with a 90-day expiration policy. This requirement does not apply to Application-to-Application Accounts or External Facing user accounts.

### **IDLE TIMEOUT**

Users are required to re-enter password after 15 minutes of idle activity.

### **ACCOUNT LOCKOUT**

User IDs shall be suspended after a maximum of six (6) failed sign-on attempts.

An account shall be suspended if an initial password remains unchanged for thirty (30) days after initial account assignment or password reset.

## **PASSWORD PROTECTION REQUIREMENTS**

Users are required to protect passwords by following these standards:

- Dynamic password tokens must not be stored in the same briefcase or suitcase as portable computers used to remotely access Telenav networks.
- If an administrator requires that you login to a machine or service, use precautions so that password(s) are not witnessed.

### **PASSWORD STORAGE**

Passwords must always be stored in encrypted form. Users should not store passwords in a file on ANY computer system (including handheld devices) without password and encryption protections.

Users should ensure that password file access is controlled from unauthorized access.

Do not write passwords down or store them anywhere other than in the authorized password vault software.

### **ENCRYPTED TRANSMISSION**

All passwords shall be transmitted utilizing strong encryption to prevent unauthorized disclosure.

### **CREDENTIAL COMMUNICATIONS**

If an account password must be communicated, a Technical Support administrator will use a secure method to convey User IDs and passwords.

## **ADMINISTRATOR PASSWORD REQUIREMENTS**

In addition to meeting all of the requirements mentioned above, administrator passwords are required to:

- Have a minimum length of twelve (12) characters.

- Include at least one (1) number, one (1) upper case character, one (1) lower case character, and one (1) special character or symbol

Administrator accounts must enforce a maximum of five (5) failed attempts before account is locked.

Administrator accounts are not allowed the use of any of the last five (5) passwords.

Administrator accounts will be configured to expire every 45 days or less.

## **PROHIBITED PASSWORD SECURITY ACTIVITIES**

There are several practices that are considered potentially dangerous to the user's system or entire network. User are expected to:

- Treat all passwords as Telenav Inc. [Restricted-Confidential] information.
- Keep passwords confidential and not share Telenav passwords with anyone, including family members, supervisor, administrative assistants, coworkers, persons claiming to be from Technical Support, Help Desk, or other official-sounding organization;
- Not reveal a password over the phone. If someone demands a password, refer them to this policy or have them call Help Desk Manager.
- Not talk about passwords in front of others;
- Not insert passwords into email messages or other forms of electronic communication;
- Not use passwords at Telenav that are the same as passwords used for personal accounts;
- Not hint at the format of a password (for example, "my family name");
- Not reveal passwords on questionnaires or security forms;
- Not reveal passwords to co-workers while on vacation or on a leave of absence;
- Not use the "Remember Password" feature within applications (e.g. Internet Explorer, Chrome)
- Not write passwords down;

## **REPORT INCIDENTS**

If accounts or passwords have been compromised, report the incident to Technical Support and change all passwords immediately.

## **LEAVING TELENNAV**

### **EMPLOYER INFORMATION AND PROPERTY**

The protection of Telenav business information, property and all other Company assets are vital to the interests and success of Telenav. No Telenav related information or property, including without limitation, documents, files, records, computer files, equipment, office supplies or similar materials (except in the ordinary course of performing duties on behalf of Telenav) may, therefore, be removed from the Company's premises. In addition, when an employee leaves Telenav, the employee must return to the Company all Telenav related information and property that the employee has in his/her possession, including without limitation, documents, files, records, manuals, information stored on a personal computer or on a computer disc, supplies, and equipment or office supplies. Violation of this policy is a serious offense and will result in appropriate disciplinary action, up to and including discharge.

### **RESIGNATION**

When an employee decides to leave for any reason, his/her supervisor and the Human Resources Department would like the opportunity to discuss the resignation before final action is taken. Telenav often finds during this conversation that another alternative may be better. If, however, after full consideration, the employee decides to leave, it is requested that the employee provide the Company with at least a written two-week advance notice period. If, as sometimes happens, the employee's supervisor wishes for the employee to leave prior to the end of the employee's notice period, the employee may be asked to leave prior to the end of notice period.

### **DISMISSALS**

Every Telenav employee has the status of "employee-at-will," meaning that no one has a contractual right, express or implied, to remain in Telenav's employ. Telenav may terminate an employee's employment, or an employee may terminate his/her employment, without cause, and with or without notice, at any time for any reason. No supervisor or other representative of the Company (except the President) has the authority to enter into any agreement for employment for any specified period of time, or to make any agreement contrary to the above.

## **EMPLOYEE CODE OF CONDUCT**

Please refer to the separate ***Telenav Code of Business Conduct and Ethics Policy*** on the Intranet.

Any employee whose conduct, actions or performance violates or conflicts with Telenav's Code of Conduct may be terminated immediately and without warning at the discretion of Telenav's management.

The following are some examples of grounds for immediate dismissal of an employee:

- Breach of trust or dishonesty
- Conviction of a felony
- Willful violation of an established policy or rule
- Falsification of Company records
- Gross negligence
- Insubordination
- Violation of the Anti-Harassment and/or Equal Employment Opportunity Policies
- Time card or sign-in book violations
- Undue and unauthorized absence from duty during regularly scheduled work hours
- Deliberate non-performance of work
- Larceny or unauthorized possession of, or the use of, property belonging to any co-worker, visitor, or customer of Telenav
- Possession of dangerous weapons on Company premises
- Unauthorized possession, use or copying of any records that are the property of Telenav
- Unauthorized posting or removal of notices from bulletin boards
- Excessive absenteeism or lateness
- Marring, defacing or other willful destruction of any supplies, equipment or property of Telenav
- Failure to call or directly contact your supervisor when you will be late or absent from work
- Fighting or serious breach of acceptable behavior
- Violation of the Company's Alcohol or Drug Policy
- Theft
- Violation of the Company's Conflict of Interest/Outside Employment Policy and/or Confidentiality Policy
- Gambling, conducting games of chance or possession of such devices on the premises or during work hours
- Leaving the work premises without authorization during work hours
- Rudeness towards customer
- Sleeping on duty

This list is intended to be representative of the types of activities that may result in disciplinary action. It is not exhaustive, and is not intended to be comprehensive and does not change the employment-at-will relationship between the employee and the Company. In the event of dismissal for misconduct, all benefits end at the end of the month. COBRA may not be available to anyone dismissed from Telenav for gross misconduct.

## **DISCIPLINE OTHER THAN IMMEDIATE DISCHARGE**

All employees are expected to meet Telenav's standards of work performance. Work performance encompasses many factors, including attendance, punctuality, personal conduct, job proficiency and general compliance with the Company's policies and procedures.

If an employee does not meet these standards, the Company may, under appropriate circumstances, take corrective/disciplinary action, other than immediate dismissal.

The intent of corrective/disciplinary action is to formally document problems while providing the employee with a reasonable time within which to improve performance. The process is designed to encourage development by providing employees with guidance in areas that need improvement such as poor work performance, attendance problems, personal conduct, general compliance with the Company's policies and procedures and/or other disciplinary problems. The Company's decision to impose corrective/disciplinary action does not change the employee's status as an at-will employee and does not constitute a guarantee of continued employment for any duration. Telenav always reserves for itself the right to terminate an employee for any reason without prior notice.

### **WRITTEN WARNINGS**

The supervisor should discuss the problem and present a written warning to the employee with the guidance of a Human Resources representative. This should clearly identify the problem and outline a course of corrective/disciplinary action within a specific time frame. The employee should clearly understand both the corrective action and the consequence (i.e., discharge) if the problem is not corrected or reoccurs. The employee should acknowledge receipt of the warning and include any additional comments before signing it. A record of the discussion and the employee's comments should be placed in the employee file in the Human Resources Department.

Employees who have had formal written warnings are not eligible for salary increases, bonus awards, promotions or transfers during the warning period.

Generally, at the Company's discretion, corrective/disciplinary action consists of a verbal warning or Performance Improvement Plan (P.I.P.) and written warnings followed by termination. The corrective/disciplinary process shall be determined on a case-by-case basis and can cease at any stage if management sees the improvements necessary from the employee.

## **POST RESIGNATION/DISCHARGE PROCEDURES**

### **BENEFITS**

Benefits (Life, Medical and Dental) generally end on the last day of the month in which your last day of employment falls, as provided by the terms of the applicable benefit plan. An employee, unless dismissed for gross misconduct, has the option to convert to individual life insurance, and/or to

continue Medical/Dental Benefits in accordance with the Consolidated Omnibus Budget Reconciliation Act ("COBRA") regulations.

### **FINAL PAYCHECK**

Final paychecks will be issued on the last day of employment, when an employee is terminated or has given at least 72 hours' notice of his or her resignation, however, checks for out of state employees may be delayed until the next regular

pay period, if state law permits. If there are unpaid obligations to the Company, upon a written authorization from the employee permitting the deduction, the final paycheck will reflect the appropriate deductions. Employees leaving the Company must return office key FOB, badges, corporate credit cards, laptop, cell phone, etc., before their final paycheck can be issued, if permitted by applicable state laws. Telenav will comply with all applicable state laws for the payment of final wages.

---

## **ACKNOWLEDGMENT OF RECEIPT OF EMPLOYEE HANDBOOK**

The Employee Handbook contains important information about the Company, and I understand that I should consult my Direct Supervisor and/or the Human Resources Manager regarding any questions not answered in the handbook. I have entered into my employment relationship with the Company voluntarily, and understand that there is no specified length of employment. Accordingly, either the Company or I can terminate the relationship at will, at any time, with or without cause, and with or without prior notice.

I understand and agree that no person other than the CEO may enter into an employment agreement for any specified period of time, or make any agreement contrary to the Company's stated employment-at-will policy.

Since the information, policies, and benefits described herein are subject to change at any time, I acknowledge that revisions to the handbook may occur, except to the Company's policy of employment-at-will. All such changes will generally be communicated through official notices, and I understand that revised information may supersede, modify, or eliminate existing policies.

Furthermore, I understand that this handbook is neither a contract of employment nor a legally-binding agreement. I have had an opportunity to read the handbook, and I understand that I may ask my supervisor or the Human Resources Department any questions I might have concerning the handbook. I accept the terms of the handbook. I also understand that it is my responsibility to comply with the policies contained in this handbook, and any revisions made to it. I further agree that if I remain with the Company following any modifications to the handbook, I thereby accept and agree to such changes.

I have received a copy of the Company's Employee Handbook and have been prompted by the Policy Library to read and acknowledge it. I understand that I am expected to read the entire handbook. Additionally, I will click and acknowledge both receipt and understanding of the content of the Handbook by the date specified in the Policy Library system.

---

Employee Signature

---

Date