



Pinnacle Special Police, Inc.



Pinnacle Security and Crime Prevention, LLC

Employee Handbook

INTRODUCTION

Introductory Statement

This handbook is designed to acquaint you with the Companies, hereinafter called Pinnacle Company Police and Pinnacle Security and Crime Prevention, and provide you with information about working conditions, employee benefits, and some of the policies affecting your employment. You should read, understand, and comply with all provisions of the handbook. It describes many of your responsibilities as an employee and outlines the programs developed by Pinnacle Company Police and Pinnacle Security and Crime prevention to benefit employees. One of our objectives is to provide a work environment that is conducive to both personal and professional growth.

No employee handbook can anticipate every circumstance or question about a policy. As Pinnacle Company Police and Pinnacle Security and Crime Prevention continues to grow, the need may arise and Pinnacle Company Police and Pinnacle Security and Crime Prevention reserves the right to revise, supplement, or rescind any polices or portion of the handbook from time to time as it deems appropriate, in its sole and absolute discretion. The only exception to any changes is our employment-at-will policy permitting you or Pinnacle Company Police or Pinnacle Security and Crime Prevention to end our relationship for any reason at any time. Employees will, of course be notified of such changes to the handbook as they occur.

I. EMPLOYMENT

101 Nature of Employment

This handbook is intended to provide employees with a general understanding of our personnel policies and is intended only as a guide for both employer and employee. Employees are encouraged to familiarize themselves with the contents of this handbook, for it will answer many common questions concerning employment with Pinnacle Company Police and Pinnacle Security and Crime Prevention.

However, this handbook cannot anticipate every situation or answer every question about employment. **It is not an employment contract and is not intended to create contractual obligations of any kind.** Neither the employee nor Pinnacle Company Police or Pinnacle Security and Crime Prevention are bound to continue the employment relationship if either chooses, at its will, to end the relationship at any time.

In order to retain necessary flexibility in the administration of policies and procedures, Pinnacle Company Police and Pinnacle Security and Crime Prevention reserves the right to change, revise or eliminate any of the policies and/or benefits described in this handbook, except for its policy of employment-at-will.

102 Equal Employment Opportunity

In order to provide equal employment and advancement opportunities to all individuals, employment decisions at Pinnacle Company Police and Pinnacle Security and Crime Prevention will be based on merit, qualifications, and abilities. Pinnacle Company Police and Pinnacle Security and Crime Prevention does not discriminate in employment opportunities or practices on the basis of race, color, religion, sex, national origin, age disability, or any other characteristic protected by law.

Pinnacle Company Police and Pinnacle Security and Crime Prevention will make reasonable accommodations for qualified individuals with known disabilities unless doing so would result in an undue hardship. This policy governs all aspects of employment, including selection, job assignment, compensation, discipline, termination, and access to benefits and training.

Any employees with questions or concerns about any type of discrimination in the workplace are encouraged to bring these issues to the attention of their immediate supervisor, the Pinnacle Company Police and Pinnacle Security and Crime Prevention Manager or Human Resources Officer at Pinnacle. Employees can raise concerns and make reports without fear of reprisal. Anyone found to be engaging in any type of unlawful discrimination will be subject to disciplinary action, up to and including termination of employment.

103 Americans With Disabilities Act

Pinnacle Company Police and Pinnacle Security and Crime Prevention are committed to complying with all applicable provisions of the Americans with Disabilities Act (“ADA”). It is Pinnacle Company Police and Pinnacle Security and Crime Prevention’s policy not to discriminate against any qualified employee or applicant with regard to any terms or conditions of employment because of such individual’s disability or perceived disability as long as the employee can perform the essential functions of the job. Consistent with this policy of nondiscrimination, Pinnacle Company Police and Pinnacle Security and Crime Prevention will provide reasonable accommodations to a qualified individual with a disability, as defined by the ADA, who has made Pinnacle Company Police and Pinnacle Security and Crime Prevention aware of his of her disability, provided that such accommodation does not constitute an undue hardship on Pinnacle Company Police or Pinnacle Security and Crime Prevention. Employees with a disability who believe they need a reasonable accommodation to perform the essential functions of their job should contact a member of Pinnacle Company Police or Pinnacle Security and Crime Prevention’s management. Pinnacle Company Police and Pinnacle Security and Crime Prevention encourage individuals with disabilities to come forward and request reasonable accommodation.

104 Employment Applications

Information given to Pinnacle Company Police or Pinnacle Security and Crime Prevention on the Employment Application or any other document by an applicant or employee is relied upon as being accurate. Any misrepresentations, falsifications, or material omission of information or data may result in termination.

105 Immigration Law Compliance

Pinnacle Company Police and Pinnacle Security and Crime Prevention is committed to employing only United States Citizens and aliens who are authorized to work in the United States and does not unlawfully discriminate on the basis of citizenship or national origin

In compliance with the immigration Reform and Control Act (IRCA) of 1986, each new employee, as a condition of employment, must complete the Employment Eligibility Verification Form I-9 and present documentation establishing identity and employment eligibility. Former employees who are rehired must also complete the form if they have not completed an I-9 with Pinnacle Company Police or Pinnacle Security and Crime Prevention within the past three years, or if their previous I-9 is no longer retained or valid.

Employees with questions or seeking more information on Immigration law issues are encouraged to contact Human Resources at Pinnacle. Employees may raise questions or complaints about immigration law compliance without fear of reprisal.

106 Conflict of Interest

No employee of Pinnacle Company Police or Pinnacle Security and Crime Prevention shall maintain an outside business or financial interest, or engage in any outside business or financial activity, which conflicts with the interest of Pinnacle Company Police or Pinnacle Security and Crime Prevention or which interferes with his or her ability to fully perform job responsibilities. For example, and not by limitation, if your job responsibilities include purchasing, or you are in a position to influence such purchases, you should have no proprietary or financial interest in any business that furnishes products, materials, or services to Pinnacle Company Police or Pinnacle Security and Crime Prevention or in any related transaction. Nor may you benefit directly or indirectly from a third party who furnishes products, materials, or services to Pinnacle Company Police or Pinnacle Security and Crime Prevention. Violation of this policy can result in immediate dismissal.

107 Outside Employment

Employees may hold outside jobs as long as they meet the performance standards of their job with Pinnacle Company Police or Pinnacle Security and Crime Prevention. All employees will be judged by the same performance standards and will be subject to Pinnacle Company Police or Pinnacle Security and Crime Prevention's scheduling demands, regardless of any existing outside work requirements.

If Pinnacle Company Police or Pinnacle Security and Crime Prevention determines that an employee's outside work interferes with performance or the ability to meet the requirements of Pinnacle Company Police or Pinnacle Security and Crime Prevention as they are modified from time to time, the employee may be asked to terminate the outside employment if he or she wishes to remain with Pinnacle Company Police or Pinnacle Security and Crime Prevention. Outside employment that constitutes a conflict of interest is prohibited. Employees may not receive any income or material gain from individual's outside Pinnacle Company Police or Pinnacle Security and Crime Prevention for materials produced or services rendered while performing their jobs at Pinnacle Company Police or Pinnacle Security and Crime Prevention.

108 Non-Disclosure

The protection of confidential information and trade secrets is vital to the interests of the success of Pinnacle Company Police and Pinnacle Security Crime Prevention. Employees who improperly use or disclose trade secrets or confidential information will be subject to disciplinary action, up to and including termination of employment and legal action, even if they do not actually benefit from the disclosed information.

II. EMPLOYMENT STATUS AND RECORDS

201 Employment Categories

It is the intent of Pinnacle Company Police and Pinnacle Security and Crime Prevention to clarify the definitions of employment classifications so that employees understand their employment status and benefit eligibility. These classifications do not promise or guarantee employment for any specified period of time. Accordingly, the right to terminate the employment relationship at will at any time is retained by both the employee and Pinnacle Company Police and Pinnacle Security and Crime Prevention.

Each employee is designated as either NONEXEMPT AND EXEMPT from federal and state wage and hour laws. NONEXEMPT employees are entitled to overtime pay under the specific provisions of federal and state laws. EXEMPT employees are excluded from specific provisions of federal and state wage and hour laws. An employee's EXEMPT or NONEXEMPT classification may be changed only upon written notification by the Pinnacle Company Police and Pinnacle Security and Crime Preventions payroll manager.

In addition to the above categories, each employee will belong to one other employment category:

REGULAR FULL-TIME employees are those who are not in a temporary or introductory status and who are regularly scheduled to work Pinnacle Company Police or Pinnacle Security and Crime Prevention full-time schedule. Generally, they are eligible for Pinnacles benefit package, subject to the terms, conditions, and limitations of each benefit program.

PART-TIME employees are those who are not assigned to a temporary or introductory status who are regularly scheduled to work 20 hours or more but less than 30 hours per week. While they do receive all legally mandated benefits (such as Social Security and workers' compensation insurance), they are ineligible for all of Pinnacles other benefit programs.

INTRODUCTORY employees are those whom their performance is being evaluated to determine whether further employment in a specific position or with Pinnacle Company Police or Pinnacle Security and Crime Prevention is appropriate. Employees who satisfactorily complete the introductory period will be notified of their new employment classification.

TEMPORARY employees are those who are hired as interim replacements, to temporarily supplement the work force, or to assist in the completion of a specific project. Employment assignments in this category are of a limited duration. Employment beyond any initially stated period does not in any way imply a change in employment status. Temporary employees retain that status unless and until notified of a change. All legally mandated benefits (such as Social Security and workers' compensation insurance) are provided to temporary employees. Pinnacle Company Police and Pinnacle Security and Crime Prevention sponsored benefits may also be available, subject to the terms, conditions, and limitations of each benefit program.

202 Access to Personnel Files

Pinnacle Company Police and Pinnacle Security and Crime Prevention maintain a personnel file on each employee. The Personnel file includes such information as the employee's job application, resume, records of training, documentation of performance appraisals and salary increases, and other employment records.

Personnel files are the property of Pinnacle Company Police and Pinnacle Security and Crime Prevention, and access to the information they contain is restricted. Another important issue is the right of employees to access their own personnel records. Unlike some states, North Carolina does not have a law giving private-sector employees the right to inspect their own employment files.

203 Employment Reference Checks

To ensure that individuals who join Pinnacle Company Police or Pinnacle Security and Crime Prevention are well qualified and have a strong potential to be productive and successful, it is the policy of Pinnacle Company Police and Pinnacle Security and Crime Prevention to check the employment references of all applicants.

The Hiring Supervisor will respond to all reference check inquiries from other employers. Responses to such inquiries will confirm only dates of employment, wage rates, and positions(s) held. No employment data will be released without a written authorization and release signed by the individual who is the subject of the inquiry.

204 Personnel Data Changes

It is the responsibility of each employee to promptly notify Pinnacle Company Police or Pinnacle Security and Crime prevention manager of any changes in personnel data. Personal mailing addresses, telephone numbers, number and names of dependents, individuals to be contacted in the event of an emergency, educational accomplishment, and other such status reports should be accurate and current at all times. If any personnel data has changed, notify the Manager or Supervisor and Human Resources Officer at the Pinnacle Corporate Office within 24 hrs.

205 Introductory Period

The Introductory period is intended to give new employees the opportunity to demonstrate their ability to achieve a satisfactory level of performance and to determine whether the new position meets their expectations. Pinnacle Company Police and Pinnacle Security and Crime Prevention use this period to evaluate employee's capabilities, work habits, and overall performance. Either the employee or Pinnacle Company Police and Pinnacle Security and Crime Prevention may end the employment relationship at will at any time during or after the introductory period, with or without cause or advance notice.

All new and rehired employees work on an introductory basis for the first 90 calendar days after their date of hire. Any significant absence will automatically extend an introductory period by the length of the absence. If Pinnacle Company Police or Pinnacle Security and Crime Prevention determine that the designated introductory period does not allow sufficient time to thoroughly evaluate the employee's performance, the introductory period may be extended for a specified period.

During the initial introductory period, new employees are eligible for worker's compensation insurance and Social Security. Introductory employees are not eligible for Family Medical Leave/Leave without pay.

206 Performance Evaluation

Supervisors and employees are strongly encouraged to discuss job performance and goals on an informal, day-to-day basis. A formal written performance evaluation may be conducted at the end of any employee's initial period of hire, known as the introductory period or from time to time at the employer's discretion.

III. EMPLOYEE BENEFIT PROGRAMS

301 Employee Benefits

Eligible employees at Pinnacle Company Police and Pinnacle Security and Crime Prevention are provided a wide range of benefits. A number of programs (such as Social Security, workers' compensation, State Disability and Unemployment Insurance) cover all employees in the manner prescribed by law.

Benefits eligibility is dependent upon a variety of factors, including employee classification. A full time employee is defined as an employee working an average of 30 hours or more per week, or 1,560 hours per year, whichever is less. Your supervisor can identify the programs for which you are eligible. Some benefit programs require, contributions from the employee, others are paid all or in part by Pinnacle Company Police or Pinnacle Security and Crime Prevention. For details on these plans, please ask your supervisor.

The following benefit programs are available to full-time employees only after the first month following the completion of 90 calendar days of service:

- Medical Insurance: Pinnacle Company Police and Pinnacle Security and Crime Prevention pay 50% of the employee's coverage on the Plan. The employee pays 50% of their premium and any premium for dependent coverage.
- Dental Insurance: Employees Pay 100% of the cost of dental coverage.
- Vision Insurance: Employees pay 100% of the cost of vision coverage.
- Life Insurance: Employee pays 100% of the cost of life insurance
- Disability insurance: Employees pay 100% of the cost of disability coverage.
- Pre-Tax "Cafeteria" Treatment of Qualified Benefits.

302 Vacation Benefits

Vacation time off with pay is available to all regular full time employees to provide opportunity for rest, relaxation, and personal pursuits. After one year of service, you will be allowed one week paid vacation time off on an annual basis, anniversary date to anniversary date, based on your average workweek.

To take vacation, employees should request approval from their supervisors at least one month in advance of the required time off. Requests will be reviewed based on a number of factors, including business needs and staffing requirement. At no time will vacation be allowed during peak operating times. Vacation time off is paid at the employee's base pay rate at the time of vacation. Vacation hours are not counted as hours worked for the purposes of calculating overtime.

Employees are encouraged to use available vacation time for rest, relaxation, and personal pursuits. In the event that available vacation time is not used by the employee's anniversary date, unused time will be forfeited.

When employment ends for any reason, vacation time earned but not taken **will not** be included in the employee's final paycheck. At the same time, vacation time taken in advance will be treated as advanced wages and will be deducted from the final paycheck.

303 Workers' Compensation Insurance

Pinnacle Company Police and Pinnacle Security and Crime Prevention provide a comprehensive workers' compensation insurance program at no cost to employees. This program covers certain injuries sustained in the course of employment that requires medical, surgical, or hospital treatment.

Employees who sustain work-related injuries will inform their supervisor immediately. No matter how minor an on-the-job injury may appear, it is important that it be reported immediately. The employee and his supervisor will fill out a report of injury. If the employee is unable to fill this report out due to being incapacitated the supervisor will fill out the report of injury and **must make** notification to the corporate office of Pinnacle Special Police, Inc. by phone **and** electronic method such as email or text notification. This will enable an eligible employee to qualify for coverage as quickly as possible.

Neither Pinnacle Company Police or Pinnacle Security and Crime Prevention nor the insurance carrier will be liable for the payment of workers' compensation benefits for injuries that occur during an employee's voluntary participation in any off-duty recreational, social, or athletic activity sponsored by Pinnacle Company Police or Pinnacle Security and Crime Prevention.

304 Time Off to Vote

Pinnacle Company Police and Pinnacle Security and Crime Prevention encourage employees to fulfill their civic responsibilities by participating in elections. Generally, employees are able to find time to vote either before or after their regular work schedule. Pinnacle Company Police and Pinnacle Security and Crime Prevention will not grant time off to vote.

305 Jury Duty or Subpoenaed for Court

We intend to be good community citizens and will accommodate summons to witness and jury duty (without compensation). Please notify your supervisor as soon as possible to allow for substitutions.

306 Benefits Continuation (COBRA)

The federal Consolidated Omnibus Budget Reconciliation Act (COBRA) gives employees and their qualified beneficiaries the opportunity to continue health insurance coverage under Pinnacle's health plan when a "qualifying event" would normally result in the loss of eligibility. Some common qualifying events are resignation, termination of employment, or death of any employee; a reduction in an employee's hours or a leave of absence; an employee's divorce or legal separation; and a dependent child no longer meeting eligibility requirements.

Under COBRA, "The employee or beneficiary pays the full cost of coverage at Pinnacle's group rates plus an administration fee. Pinnacle provides each eligible employee with a written notice describing rights granted under COBRA when the employee becomes eligible for coverage under Pinnacle's health insurance plan. The notice contains important information about the employee's right and obligations.

307 Group Health and Dental Insurance

Pinnacle Company Police and Pinnacle Security and Crime Prevention through Pinnacle's health and dental insurance plan, provides its employees and their dependents access to medical, prescription drug, dental and vision discount care benefits. Employees in the following employment classifications are eligible to participate in the health and dental insurance plans:

- Regular full-time employees that work an average of 30 hours per week during the prior year.

Eligible employees may participate in the health insurance plan subject to all terms and conditions of the agreement between Pinnacle and the insurance carrier and/or administrator. Eligible employees may participate in health and dental insurance coverage only after the first of the month following the completion of 90 calendar days of service.

A change in employment classification that would result in the loss of eligibility to participate in the health insurance plan may qualify an employee for benefits continuation under the Consolidated Omnibus Budget Reconciliation Act (COBRA). Refer to the Benefits Continuation (COBRA) policy for more information.

Details of the health and dental insurance plan are described in the Summary Plan Description (SPD). A SPD and information on cost of coverage will be provided in advance of enrollment to eligible employees, Contact the Human Resources Department at Pinnacle for more information about the health and dental insurance benefits.

308 Life Insurance

Life insurance offers you and your family important financial protection. Pinnacle Company Police and Pinnacle Security and Crime Prevention through our insurance, provide a basic term life insurance plan for eligible employees.

Additional supplemental and/or dependent term life insurance coverage may also be purchased.

Employees in the following employment classifications are eligible to participate in the life insurance plan:

- Regular full-time employees that work an average of 30 hours per week during the prior year.

Eligible employees may participate in the life insurance plan subject to all terms and conditions of the agreement between Pinnacle and the insurance carrier. Eligible employees may participate in life insurance coverage only after the first of the month following the completion of 90 calendar days of service.

Details of the basic term life insurance plan including benefit amounts are described in the Summary Plan Description provided to eligible employees. Contact the Human Resources Department at Pinnacle for more information about life insurance benefits.

309 Long-Term Disability

Pinnacle Company Police and Pinnacle Security and Crime Prevention through Pinnacle insurance provides a long-term disability (LTD) benefits plan to help eligible employees cope with an illness or injury that results in a long-term absence from employment. LTD is designed to ensure a continuing income for employees who are disabled and unable to work.

Employees in the following employment classifications are eligible to participate in the health insurance plan:

- Regular full-time employees that work an average of 30 hours per week during the prior year.

Eligible employees may participate in the LTD plan subject to all terms and conditions of the agreement between Pinnacle and the insurance carrier. Eligible employees may begin

LTD coverage only after the first of the month following the completion of 90 calendar days of service.

LTD benefits are offset with amounts received under Social Security or workers' compensation for the same time period,

Details of the LTD benefits plan including benefit amounts, and limitations and restrictions are described in the Summary Plan Description provided to eligible employees. Contact the Human Resources Department at Pinnacle for more information about LTD benefits.

310 Employee Parking

Employees should park in areas designed at each location. Parking spots located near entrances should remain available for guests. Any employee with a valid handicapped placard will be allowed to use the handicapped parking.

IV. TIMEKEEPING/PAYROLL

401 Timekeeping

Every consideration for accommodating employee requests will be considered when establishing work schedules. Employees are expected to adhere to posted work schedules and avoid absenteeism and tardiness. Repeated offenses are grounds for disciplinary action, up to and including termination.

Accurately recording time worked is the responsibility of every nonexempt/hourly paid employee. Federal and state laws require Pinnacle Company Police and Pinnacle Security and Crime Prevention to keep an accurate record of time worked in order to calculate employee pay and benefits. Time worked is all the time actually spent on the job performing assigned duties.

Nonexempt/hourly paid employees should accurately record the time they begin and end their work, as well as the beginning and ending time of each meal period. They should also record the beginning and ending time of any split shift or departure from work for personal reasons. Overtime work must always be approved before it is performed. Failure to obtain approval will be treated as willful misconduct and could result in disciplinary action up to and including termination.

Altering, falsifying, tampering with time records, failing to clock in or clock out, or recording time on another employee's time record may result in disciplinary action, up to and including termination of employment.

The supervisor will review and the initial the time record before submitting it for payroll processing. In addition, if corrections or modifications are made to the time record, both the employee and the supervisor must verify the accuracy of the changes by initialing the time record.

Some of our operations are open 24 hours a day, seven days a week, year round. As a security business, we strive to serve our clients at all times, including holidays, employees will be required to work holidays as necessary. Every effort will be made to fairly distribute holiday time off. At no time will exceptions be made for any holiday or local event that will attract high volumes of business.

402 Paydays

All employees are paid every other Friday. Each paycheck will include earnings for all work performed through the end of the payroll period.

In the event that a regularly scheduled payday falls on a holiday (Christmas), employees will receive their paycheck the day before the regularly scheduled payday (based on Pinnacle's holiday payroll processing schedule).

In the event that an employee's paycheck is lost or stolen an employee should notify their supervisor immediately. The supervisor will notify the payroll manager at Pinnacle who will attempt to put a stop payment notice on the employee's check. There is a \$25 stop payment fee, as well as a \$25 fee to issue a replacement check, which will be deducted from the employee's replacement check.

403 Employment Terminations

Termination of employment is an inevitable part of personnel activity within any organization, and many of the reasons for termination are routine. Below are examples of some of the most common circumstances under which employment is terminated.

- **Resignation** - voluntary employment termination initiated by an employee.
- **Discharge** - Involuntary employment termination initiated by the organization.
- **Layoff** - Involuntary employment termination initiated by the organization for non-disciplinary reasons.
- **Retirement** - Voluntary employment termination initiated by the employee meeting age, length of service, and any other criteria for retirement from the organization.

Since employment with Pinnacle Company Police or Pinnacle Security and Crime Prevention is based on mutual consent both the employee and Pinnacle Company Police or Pinnacle Security and Crime Prevention have the right to terminate employment at

will, with or without cause, at any time. Employees will receive their final pay in accordance with applicable state law.

Employee benefits will be affected by employment termination in the following manner.

- All accrued, vested benefits that are due and payable at termination will be paid.
- Pinnacle Company Police and Pinnacle Security and Crime Prevention does not pay for accrued unused vacation at termination,
- Some benefits may be continued at the employee's expense if the employee so chooses.

The employee will be notified in writing of the benefits that may be continued and of the terms, conditions, and limitations of such continuance.

404 Pay Advances

Pinnacle Company Police and Pinnacle Security and Crime Prevention do not provide pay advances on unearned wages to employees. Also no advances will be made if you owe money to the company for training or equipment purchases.

405 Administrative Pay Corrections

Pinnacle Company Police and Pinnacle Security and Crime Prevention will take all reasonable steps to ensure that employees receive the correct amount of pay in each paycheck and that employees are paid promptly on the scheduled payday.

In the unlikely event that there is an error in the amount of pay, the employee should promptly bring the discrepancy to the attention of the Pinnacle Payroll Department so that correction can be made as quickly as possible. The telephone number for Pinnacle Company Police and Pinnacle Security and Crime Prevention is 910-798-8586.

If you receive an answering machine or service please leave a message stating your problem. Depending on the nature of the problem the amount in error will be corrected on the next paycheck. Please report the problem to your manager and follow proper policies.

406 Pay Deductions and Setoffs

The law requires that Pinnacle make certain deductions from every employee's compensation. Among these are applicable federal, state and local income taxes. Pinnacle also must deduct Social Security Taxes on each employee's earnings up to a specified limit that is called the Social Security "wage base". Pinnacle matches the amount of Social Security taxes paid by each employee.

Pinnacle Company Police and Pinnacle Security and Crime Prevention offers programs and benefits beyond those required by law. Eligible employees may voluntarily authorize deductions from their pay checks to cover the costs of participation in these programs.

V. WORK CONDITIONS AND HOURS

501 Safety

To assist in providing a safe and healthful work environment for employees, customers, and visitors Pinnacle Company Police and Pinnacle Security and Crime Prevention has established workplace safety as a top priority. Pinnacle Company Police and Pinnacle Security and Crime prevention have a responsibility for implementing, administering, monitoring and evaluating safety in the workplace. Our success depends on the alertness and personal commitment of all.

Pinnacle Company Police and Pinnacle Security and Crime Prevention provide information to employees about workplace safety and health issues through regular internal communication channels such as staff meetings, bulletins board postings, memos, meetings or other communications.

Some of the best safety improvement ideas come from employees. Those with ideas, concerns, or suggestions for improved safety in the workplace are encouraged to share them with their supervisor, or bring them to the attention of Pinnacle Company Police and Pinnacle Security and Crime Prevention Supervisors or Managers. Reports and concerns about workplace safety issues may be made anonymously if the employee wishes. All reports can be made without fear of reprisal.

Each employee is expected to obey safety rules and to exercise caution in all work activities. This includes wearing personal protective devices for vision, hearing, breathing and other needs as provided by Pinnacle Company Police or Pinnacle Security and Crime Prevention. All protective shields on equipment are to be in place during operations or as prescribed by the equipment instructions. All other safety devices should be fully utilized and employees who fail to utilize such devices are subject to disciplinary action up to and including termination. Employees must immediately report any unsafe condition to the appropriate supervisor. Employees who violate safety standards, who cause hazardous or dangerous situations, or who fail to report or, where appropriate, remedy such situations, may be subject to disciplinary action, up to an including termination of employment.

In the case of accidents that result in injury, regardless of how insignificant the injury may appear, employees should notify the appropriate supervisor immediately. Such reports are necessary to comply with laws and initiate insurance and workers' compensation benefit procedures. Pinnacle Company Police and Pinnacle Security and Crime Prevention supervisors or managers will be responsible for notifying Pinnacle Corporate Offices. A report of injury must be filled out by the supervisor or manager.

General Safety Rules:

1. Job safety is the responsibility of each employee. This often means applying common sense to a situation. Use good common sense and stay alert at all times.
2. All injuries, no matter how minor, must be reported to your supervisor immediately.
3. Submitting false or fraudulent information related to workplace safety will be cause for dismissal and potential denial of medical and wage loss benefits.
4. Report any unsafe conditions to you supervisor immediately, regardless of whether the unsafe condition directly affects you.
5. If at any time you are unsure how to perform the job you have been asked to do, **STOP AND CHECK WITH YOUR SUPERVISOR.** This is for you safety and that of your coworkers.
6. Do not attempt to repair or tamper with equipment that is not working properly. Please contact your supervisor.
7. Any employee who is furnished with safety equipment will be required to use such equipment.
8. Good housekeeping procedures should be followed at all times. This includes clean tools, dry floors, neat work areas, and properly arranged materials
9. Use the correct method of lifting objects. Lift with your legs, not your back. If a load is too heavy or awkward, ask for assistance.
10. Do Not Use flammable liquids, toxic materials chemicals, or acids unless Authorized and instructed in the proper procedures.
11. Do not smoke in areas that are not specifically designed as smoking areas. **SMOKING IS PROHIBITED IN GUEST ROOMS, FOOD PREPARATION AREAS, PUBLIC AREAS INCLUDING HALLWAYS, ELEVATORS, AND LOBBY (STATE AND COUNTY ORDINANCES).**
12. Obey safety and warning signs at all times.
13. Footwear must cover the entire foot and have a non-slip sole.
14. Fire drills will be conducted on a regular basis.
15. If working a motel, guest security is first.
Do not allow guest into guest rooms with your pass key.
If they are a registered guest they should have a guest room key; if not, direct them to the front desk for assistance. Do not block any exterior doors at any time.
16. To ensure guest security, under no circumstances should guest information, Including guest room number, be provided to anyone.

502 Use of Phone, Mail and Internet Systems

Personal use of telephones for long-distance and toll calls is not permitted. Employees should practice extreme discretion in using company telephones when making local personal calls, limiting the calls to breaks or meal periods. Also, personal use of the Internet, electronic mail (“e-mail”), and the postage system is not permitted. Personal use of the company’s 1-800 numbers is strictly prohibited.

Employees will be required to reimburse Pinnacle Company Police and Pinnacle Security and Crime Prevention for any charges resulting from their personal use of the telephone, the Internet, and/or mail systems.

Personal cell phone usage by employees is permitted but should be limited to short conversations so the officer is not distracted from duty.

Unauthorized use of the Pinnacle telephone for personal use and/or any personal use of the Internet and/or mail systems will be considered willful misconduct and may result in disciplinary action, up to and including, termination.

503 Smoking

In keeping with Pinnacle Company Police and Pinnacle Security and Crime Prevention's intent to provide a safe and healthful work environment, smoking is not permitted while in uniform.

504 Rest and Meal Periods

Each workday, full-time nonexempt hourly employees are provided with 2 rest periods of 10 minutes in length. To the extent possible, rest periods will be provided in the middle of work periods. Since this time is counted and paid as time worked, employees must not be absent from their workstations beyond the allotted rest period time.

All full-time employees are permitted a 30 minute unpaid meal break after four (4) continuous work hours. Supervisors will schedule meal periods to accommodate operating requirements. Employees will be relieved of all responsibilities during meal periods and will not be compensated for that time. Employees must punch out for their meal period.

505 Violence in The Workplace

Pinnacle Company Police and Pinnacle Security and Crime Prevention 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, Pinnacle Company Police and Pinnacle Security and Crime Prevention's company manager and/or the Human Resources department at pinnacle Corporation. All complaints will be fully investigated.

Pinnacle Company Police and Pinnacle Security and Crime Prevention will promptly respond to any incident or suggestion of violence. Violation of this policy will result in disciplinary action, up to and including termination of employment.

VI. LEAVE OF ABSENCE

601 Family Medical Leave Act (FMLA)

Under the family and medical Leave Act of 1992 (FMLA), eligible employees may be granted up to a total of 12 weeks of unpaid leave per 12-month period, as determined below, for any of the following reasons: (i) birth of the employee's child or to care for the newborn child; (ii) the placement of a child with the employee for adoption or foster care or to care for the newly placed child; (iii) to care for the employee's child, spouse, or parent (but not in-law) with a serious health condition; or (iv) the employee's own serious health condition that makes the employee unable to perform one or more of the essential functions of his or her job. A "serious health condition means an illness, injury, impairment, or physical or mental condition that involves inpatient care in a hospital, hospice, or residential medical care facility; or continuing treatment by a health care provider.

Employees who have worked for PINNACLE COMPAY POLICE AND PINNACLE SECURITY AND CRIME PREVENTION for at least one year and a minimum of 1,250 hours in the twelve months proceeding the request may be eligible for up to 12 weeks of leave during a rolling twelve month period,. For the purposes of determining available leave, the 12- month period during which employees may be eligible for leave will be calculated on rolling 12- month period measured backwards from the date the employee is requesting leave.

Employees requesting leave must obtain the appropriate forms from Pinnacle Company Police and Pinnacle Security and Crime Prevention 's company manager or the Pinnacle Human Resources Department and submit the completed forms to their supervisor at least 30 days in advance of foreseeable events and as soon as possible for unforeseeable events.

Employees requesting family leave related to the serious health condition of a child, spouse, or parent may be required to submit a health care provider's statement verifying the need for a family leave to provide care, its beginning and expected ending dates, and the estimated time required.

An eligible employee is entitled up to 12 workweeks of unpaid leave during a 12-month period for any FMLA qualifying reasons(s). Employees will be required to first use any accrued paid leave time as part of that 12 week period before going on unpaid family leave. Married employee couples may be restricted to a combined total of 12 weeks leave within any 12-month period for childbirth, adoption, or placement of foster child; or to care for a parent with a serious health condition.

Employees may continue health care coverage under the group health plan during the leave on the same terms and conditions as would have applied had they not taken the leave, Employees who fail to return from leave may be required to repay to Pinnacle

Company Police and Pinnacle Security and Crime Prevention any premiums it paid to maintain their benefits coverage during the leave.

Benefit accruals, such as vacation, sick leave, or holiday benefits will be suspended during the leave and will resume upon return to active employment.

So that an employee's return to work can be properly scheduled, an employee on family leave is requested to provide Pinnacle Company Police or Pinnacle Security and Crime Prevention with at least two weeks advance notice of the date the employee intends to return to work,. When a family leave ends, the employee will be reinstated to the same position, if it is available, or to an equivalent position for which the employee is qualified.

If an employee fails to return to work on the agreed upon return date, Pinnacle Company Police or Pinnacle Security and Crime Prevention will assume that the employee has resigned.

V11. EMPLOYEE CONDUCT AND DISCIPLINARY ACTION

701 Employee Conduct and Work Rules

All employees are expected to present a friendly and cooperative demeanor to all clients, guests, visitors and fellow employees. Even when confronted with an abusive person, like behavior will not be tolerated. Remember, the customer is the reason we are in business. Failure to respond in a courteous manner may result in disciplinary action, up to and including, termination.

Pinnacle Company Police and Pinnacle Security and Crime Prevention should be a safe and pleasant place to work. It is important that employees understand their individual misconduct or poor performance could impact the quality and quantity not only of their work but the work of others, customers and Pinnacle Company Police and Pinnacle Security and Crime Prevention as a whole. To help you understand the expectations, stated below is a partial list of behaviors that are considered to be improper and willful misconduct.

Demonstrating behaviors such as these will result in discipline up to and including discharge. This list should not be considered all-inclusive. It is your responsibility to be familiar with and understand specific rules and standards that might apply to that location or department in order to avoid violations.

1. Willful or negligent damage, destruction, misuse, or theft of property belonging to Pinnacle Company Police or Pinnacle Security and Crime Prevention, other employees, customers or any other party.
2. Failure to meet and adhere to your specific work schedule. Changes to your work schedule must be approved by your supervisor.

3. Horseplay fighting, disorderly or loud conduct, lewd, profane or improper language.
4. Threats of violence, or using abusive language.
5. Failing to meet deadlines, neglecting duties, sleeping or loafing.
6. Possession, use, or being under the influence of alcohol, drugs, narcotics, or possession of paraphernalia associated with the use of drugs or narcotics.
7. Possession of a weapon of any type on Company premises, or possession of a weapon in company or personal vehicles while on the clock without the express written permission or authorization of Pinnacle. Officers who are certified to carry a firearm by the NC Private Protective Services Board or certified to carry weapons such as impact weapons or Tasers will be exempt from this policy.
8. Falsification of time records, allowing another person to falsify time records or the falsification of any Company records or information provided to Pinnacle Company Police and Pinnacle Security and Crime Prevention, including but not limited to, information requested to obtain employment, to change work duties or to take time off.
9. Disrespect, foul language, belligerence, disobedience or insubordination toward your supervisor or management.
10. Distribution of written or printed non-work materials of any kind in work areas or in non-work areas during work time.
11. Habitual, willful or negligent violations of workplace safety or health regulations.
12. Solicitation of any kind on Company property during work time.
13. Smoking.
14. Harassment of any employee, customer, client, or vendor either orally, physically, sexually or otherwise.
15. Wearing clothing, jewelry or other personal items that is inconsistent with workplace safety or accepted business standards.
16. Any discrimination against another employee on the basis of race, color, age, creed, national origin, sex, disability, or other protected classes of individuals.
17. Taking part in or being involved in any illegal activity either on or off the clock.
18. Impoliteness, rudeness, insolence or otherwise failing to observe polite courtesies with customers or co-workers.
19. Socializing or fraternizing with or dating anyone while on company property or company time.
20. Entering guest rooms at a motel contract without an assigned tasks or business Need.

Additionally, employees should discourage personal visits while on the job. If a visit is necessary, notify your supervisor, and meet the visitor in the lobby area of a contract. Please keep these visits brief and to a minimum. At no time should visits be conducted in guest rooms.

702 Drug Free Workplace Policy

It is Pinnacle Company Police and Pinnacle Security and Crime Prevention's desire to provide a drug-free, healthful, and safe workplace. To promote this goal, employees are

required to report to work in appropriate mental and physical condition to perform their jobs in a satisfactory manner.

While on company premises and while conducting business-related activities off company premises, no employee may use, possess, distribute, sell or be under the influence of alcohol or illegal drugs. The legal use of prescribed drugs is permitted on the job only if it does not impair an employee's ability to perform the essential functions of the job effectively and in a safe manner that does not endanger other individuals in the workplace.

Violations of this policy may lead to disciplinary action, up to and including immediate termination of employment, and/or required participation in a substance abuse rehabilitation or treatment program. Such violations may also have legal consequences.

Employees with questions or concerns about substance dependency or abuse are encouraged to discuss these matters with their supervisor or Pinnacle Company Police or Pinnacle Security and Crime Prevention manager to receive assistance or referrals to appropriate resources in the community.

Employees with drug or alcohol problems that have not resulted in, and are not the immediate subject of, disciplinary action may participate in a rehabilitation or treatment program through the employee's health insurance benefit coverage (as long as the employee is currently participating in the health insurance benefit coverage).

In order to encourage employees who may have a problem with drug or alcohol use to seek assistance voluntarily, the following is a representative sampling of local drug and alcohol rehabilitation facilities:

- National Clearinghouse for Alcohol and Drug Information (Monday through Friday) – 1800-729-6686.
- National Council on Alcoholism and Drug Dependence (7 days/week 24 hours/day) – 1800-622-2255.
- Cocaine Help Line (Monday through Friday) – 1-800-COCAINE.

For more information, consult your Yellow Pages for the nearest Alcoholics Anonymous or Narcotics Anonymous office.

Employees with questions on this policy or issues related to drug or alcohol use in the workplace should raise their concerns with their supervisor or Pinnacle Company Police and Pinnacle Security and Crime Prevention company manager without fear of reprisal.

703 Sexual and Other Unlawful Harassment

Pinnacle Company Police and Pinnacle Security and Crime Prevention is committed to providing a work environment that is free from all forms of discrimination and conduct that can be considered harassing, coercive, or disruptive, including sexual harassment.

Actions, words, jokes, or comments based on an individual's sex, race, color, national origin, age, religion, disability, sexual orientation, or any other legally protected characteristic will not be tolerated.

If you experience or witness sexual or other unlawful harassment in the workplace, report it immediately to your supervisor. If the supervisor is unavailable or you believe it would be inappropriate to contact that person, you should immediately contact Pinnacle Company Police or Pinnacle Security and Crime Prevention's Manager, the Human Resources Director at the Pinnacle Corporate Offices or any other member of management. You can raise concerns and make reports without fear of reprisal or retaliation.

704 Grievance Procedure

If an individual feels that they are being subjected to unlawful treatment in the workplace, it is their responsibility and obligation to immediately report the behavior to any of the following parties:

- The Human Resources Director at Pinnacle. You may contact the HR Director by calling 1-910-798-8586; or
- Your immediate supervisor.

705 Personal Appearance

Dress grooming and personal cleanliness standards contribute to the morale of all employees and affect the professional image Pinnacle Company Police and Pinnacle Security and Crime Prevention presents to customers and visitors.

Employees should wear proper uniforms and business attire that is suitable for the job being performed. In addition, employees should dress in a manner that supports safety and health rules. Excessive make-up, jewelry and/or hazardous fashions are prohibited.

If an employee works at a location that requires uniforms, dress according to uniform policy. Managers reserve the right to define appropriate business attire and to modify the definition according to the changing business environment. If an employee is required to wear a uniform, an employee may not be allowed to work their scheduled shift if not in proper uniform.

Uniforms issued by Pinnacle Company Police and Pinnacle Security and Crime Prevention are the property of Pinnacle Company Police and Pinnacle Security and Crime Prevention. Uniforms should be worn primarily for work, and under no circumstances worn while working another job for another employer. All uniforms must be returned upon separation of employment. Failure to do so may result in deductions from final pay for non-returned uniforms.

706 Return of Property

Employees are responsible for all property, materials or written information issued to them or in their possession or control. Employees must return all property belonging to Pinnacle Company Police or Pinnacle Security and Crime Prevention immediately upon request or upon termination of employment. Where permitted by applicable laws, the employee agrees that Pinnacle Company Police and Pinnacle Security and Crime Prevention may withhold from the employee's wages or paycheck the cost of any items that are not returned when requested. Pinnacle Company Police and Pinnacle Security and Crime Prevention may also take any action deemed appropriate to recover or protect its property and the employee agrees to pay all costs of collecting these items including reasonable attorney's fees and court costs incurred by Pinnacle Company Police or Pinnacle Security and Crime Prevention.

707 Client Complaints

When things go wrong with a client, guest or visitor, try to resolve the problem yourself. Remember, client satisfaction is the only product we sell. **Clients do not like to be passed along**, so take care of the problem before it becomes a bigger and more difficult situation. If you still do not have a satisfactory disposition of the matter, you may take it to the General Manager. For best results, follow the chain of command, checking the organizational chart.

708 Resignation

Resignation is a voluntary act initiated by the employee to terminate employment with Pinnacle Company Police or Pinnacle Security and Crime Prevention. Although advance notice is not required, Pinnacle Company Police and Pinnacle Security and Crime Prevention request at least two (2) weeks' written resignation notice from all employees so that the Company does not suffer a hardship.

Failure to report to work for three (3) consecutive days is considered job abandonment and voluntary resignation by the employee.

Employees who fail to provide adequate notice of resignation are not eligible for rehire.

709 Exit Interview

Exit interviews will be conducted when possible by management. The employee's cooperation is valued in order to determine the cause for leaving Pinnacle Company Police or Pinnacle Security and Crime Prevention, and to solicit information from the terminating employee for the betterment of the company, also so the company may complete paperwork for final pay and to collect all company owned property from employees.

710 Security Inspections

Pinnacle Company Police and Pinnacle Security and Crime Prevention wishes to maintain a work environment that is free of illegal drugs, alcohol, firearms, explosives, or other improper materials. To this end, Pinnacle Company Police and Pinnacle Security and Crime Prevention prohibit the possession, transfer, sales, or use of such materials on its premises. Pinnacle Company Police and Pinnacle Security and Crime Prevention require the cooperation of all employees in administering this policy.

Desks, lockers, and other storage devices may be provided for the convenience of employees but remains the sole property of Pinnacle Company Police and Pinnacle Security and Crime Prevention. Accordingly, they, as well as any articles found within them, can be inspected by any agent or representative of Pinnacle Company Police or Pinnacle Security and Crime Prevention at any time, either with or without prior notice. It is important that the employee understand that there is no “presumption of privacy” extended to the employee at the workplace.

Pinnacle Company Police and Pinnacle Security and Crime Prevention, likewise, wish to discourage theft or unauthorized possession of this property by employees, Pinnacle Company Police or Pinnacle Security and Crime Prevention, visitors, and customers. To facilitate enforcement of this policy, Pinnacle Company Police and Pinnacle Security and Crime Prevention or its representative may inspect not only desks and lockers but also persons entering and/or leaving the premises and any packages or other belongings. Any employee who wishes to avoid inspection of any articles or materials should not bring such items onto Pinnacle Company Police and Pinnacle Security and Crime Prevention’s premises or on contracted properties.

711 Solicitation

In an effort to ensure a productive and harmonious work environment, persons employed by Pinnacle Company Police or Pinnacle Security and Crime Prevention may not solicit or distribute literature in the workplace at any time for any purpose.

Pinnacle Company Police and Pinnacle Security and Crime Prevention recognize that employees may have interests in events and organizations outside the workplace. However, employees may not solicit or distribute literature concerning these activities during work hours. (Work hours does not include lunch periods, work breaks, or any other periods in which employees are not on duty.)

In addition, the posting of written solicitations on company bulletin boards is prohibited. Bulletin boards are reserved for official organization communications.

712 Discipline

Pinnacle Company Police and Pinnacle Security and Crime Preventions' own best interest lies in ensuring fair treatment of all employees and in making certain that disciplinary actions are prompt, uniform, and impartial. Often disciplinary action is to correct the problem, prevent recurrence, and prepare the employee for satisfactory service in the future.

Employment with Pinnacle Company Police and Pinnacle Security and Crime Prevention is based on mutual consent and both the employee and Pinnacle Company Police and Pinnacle Security and Crime Prevention have the right to terminate the employment relationship at will, with or without cause or advance notice.

VIII. COMPUTER POLICES

800 Remote Access Policy

The purpose of this policy is to define standards for connecting to Pinnacle Company Police and Pinnacle Security and Crime Prevention's network from any host. These standards are designed to minimize the potential exposure to Pinnacle Company Police and Pinnacle Security and Crime Prevention from damages which may result from unauthorized use of Pinnacle Company Police and Pinnacle Security and Crime Prevention resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Pinnacle Company Police and Pinnacle Security and Crime Prevention internal systems, etc. This policy applies to all Pinnacle Company Police and Pinnacle Security and Crime Prevention employees, contractors, vendors and agents with a Pinnacle Company Police and Pinnacle Security and Crime Prevention-owned or personally-owned computer or workstation used to connect to the Pinnacle Company Police and Pinnacle Security and Crime Prevention network. This policy applies to remote access connections used to do work on behalf of Pinnacle Company Police and Pinnacle Security and Crime Prevention, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

801 General

1. It is the responsibility of Pinnacle Company Police and Pinnacle Security and Crime Prevention employees, contractors, vendors and agents with remote access privileges to Pinnacle Company Police and Pinnacle Security and Crime Prevention's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Pinnacle Company Police and Pinnacle Security and Crime Prevention.
2. General access to the Internet for recreational use by immediate household members through the Pinnacle Company Police and Pinnacle Security and Crime

- Prevention Network on personal computers is permitted for employees that have flat-rate services. The Pinnacle Company Police and Pinnacle Security and Crime Prevention employee is responsible to ensure the family member does not violate any Pinnacle Company Police and Pinnacle Security and Crime Prevention policies, does not perform illegal activities, and does not use the access for outside business interests. The Pinnacle Company Police and Pinnacle Security and Crime Prevention employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Pinnacle Company Police and Pinnacle Security and Crime Prevention's network:
 - a. *Acceptable Encryption Policy*
 - b. *Virtual Private Network (VPN) Policy*
 - c. *Wireless Communications Policy*
 - d. *Acceptable Use Policy*
 4. For additional information regarding Pinnacle Company Police and Pinnacle Security and Crime Prevention's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

802 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Pinnacle Company Police and Pinnacle Security and Crime Prevention employee provide their login or email password to anyone, not even family members.
3. Pinnacle Company Police and Pinnacle Security and Crime Prevention employees and contractors with remote access privileges must ensure that their Pinnacle Company Police and Pinnacle Security and Crime Prevention-owned or personal computer or workstation, which is remotely connected to Pinnacle Company Police and Pinnacle Security and Crime Prevention's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Pinnacle Company Police and Pinnacle Security and Crime Prevention employees and contractors with remote access privileges to Pinnacle Company Police and Pinnacle Security and Crime Prevention's corporate network must not use non-Pinnacle Company Police and Pinnacle Security and Crime Prevention email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Pinnacle Company Police and Pinnacle Security and Crime Prevention business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Pinnacle Company Police and Pinnacle Security and Crime Prevention network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to Pinnacle Company Police and Pinnacle Security and Crime Prevention internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to Pinnacle Company Police and Pinnacle Security and Crime Prevention's networks must meet the requirements of Pinnacle Company Police and Pinnacle Security and Crime Prevention-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Pinnacle Company Police and Pinnacle Security and Crime Prevention production network must obtain prior approval from Remote Access Services and InfoSec.

803 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

804 Acceptable Use Policy

Pinnacle Company Police and Pinnacle Security and Crime Prevention's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Pinnacle Company Police and Pinnacle Security and Crime Prevention established culture of openness, trust and integrity. Pinnacle Company Police and Pinnacle Security and Crime Prevention is committed to protecting Pinnacle Company Police and Pinnacle Security and Crime Prevention's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Pinnacle Company Police and Pinnacle Security and Crime Prevention. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Pinnacle Company Police and Pinnacle Security and Crime Prevention employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at Pinnacle Company Police and Pinnacle Security and Crime Prevention. These rules are in place to protect the employee and Pinnacle Company Police and Pinnacle Security and Crime Prevention. Inappropriate use exposes Pinnacle Company Police and Pinnacle Security and Crime Prevention to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Pinnacle Company Police and Pinnacle Security and Crime Prevention, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Pinnacle Company Police and Pinnacle Security and Crime Prevention.

804-A General Use and Ownership

1. While Pinnacle Company Police and Pinnacle Security and Crime Prevention's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Pinnacle Company Police and Pinnacle Security and Crime Prevention. Because of the need to protect Pinnacle Company Police and Pinnacle Security and Crime Prevention's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Pinnacle Company Police and Pinnacle Security and Crime Prevention.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. Pinnacle Company Police and Pinnacle Security and Crime Prevention recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Pinnacle Company Police and Pinnacle Security and Crime Prevention's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Pinnacle Company Police and Pinnacle Security and Crime Prevention's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within Pinnacle Company Police and Pinnacle Security and Crime Prevention may monitor equipment, systems and network traffic at any time, per Pinnacle Company Police and Pinnacle Security and Crime Prevention's Audit Policy.
5. Pinnacle Company Police and Pinnacle Security and Crime Prevention reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

804-B Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K and WinXP users) when the host will be unattended.
4. Use encryption of information in compliance with Pinnacle Company Police and Pinnacle Security and Crime Prevention's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a Pinnacle Company Police and Pinnacle Security and Crime Prevention email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Pinnacle Company Police and Pinnacle Security and Crime Prevention, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Pinnacle Company Police and Pinnacle Security and Crime Prevention Internet/Intranet/Extranet, whether owned by the employee or Pinnacle Company Police and Pinnacle Security and Crime Prevention, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

804-C Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Pinnacle Company Police and Pinnacle Security and Crime Prevention authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Pinnacle Company Police and Pinnacle Security and Crime Prevention-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Pinnacle Company Police and Pinnacle Security and Crime Prevention.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Pinnacle Company Police and Pinnacle Security and Crime Prevention or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Pinnacle Company Police and Pinnacle Security and Crime Prevention computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Pinnacle Company Police and Pinnacle Security and Crime Prevention account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to Pinnacle Company Police and Pinnacle Security and Crime Prevention is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Pinnacle Company Police and Pinnacle Security and Crime Prevention employees to parties outside Pinnacle Company Police and Pinnacle Security and Crime Prevention.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Pinnacle Company Police and Pinnacle Security and Crime Prevention's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Pinnacle Company Police and Pinnacle Security and Crime Prevention or connected via Pinnacle Company Police and Pinnacle Security and Crime Prevention's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

805 P2P File-sharing Policy

As an addendum to the company's Acceptable Use Policy—which details the utilization of the company network, the Internet, e-mail, and employees' personal computers—this policy prohibits the use of Peer-to-Peer (P2P) file-sharing applications and goes into effect immediately.

The company's goal with this additional policy is to:

- Realize the maximum productivity from each employee.
- Address any potential liability from instances when employees download copyrighted material.
- Minimize network disruption.
- Protect the network from exposure to malicious code (worm, virus, Trojan horse).
- Protect the company's intellectual property.

Here is an explanation of each issue as it relates to file-sharing applications and our company:

Worker productivity

The ongoing health of the company is contingent upon each worker giving each task his or her maximum attention and effort. Using a file-sharing application to search for files, downloading them onto the company network or a client machine, and reading or playing them at a workstation is not germane to an employee's job duties and does not enhance a worker's productivity. Another issue is the possibility that P2P applications could disrupt software on an employee's workstation.

Liability

Although many materials have been placed on P2P networks with a creator's consent, much of the material (images, software, movies, music, video) has been duplicated from copyrighted materials. Downloading such files onto the company network or a client machine places the company at significant risk for legal action by the copyright holder and other organizations. File-sharing networks also provide ready access to pornography or other offensive material, subjecting the company and its employees to additional legal risk.

Network disruption

Although the company has sufficient Internet bandwidth to accommodate all business-related activity, performance can degrade significantly when P2P file-sharing applications are used, especially when large files are being downloaded. This problem is compounded when other users on the P2P network use company bandwidth to download files from the employee's computer, which can greatly slow other services, such as e-mail, Web browsing, and—more significantly—e-commerce on the company Web site.

Security

P2P networks can introduce serious gaps in an otherwise secure network. Threats such as worms and viruses can easily be introduced into the company's network. P2P applications, if modified, can also allow users outside the company to gain access to data on the employee's computer or even the corporate network. (Although most P2P applications allow users to disable file-sharing, such measures do little to prevent threats from being downloaded onto a user's machine.) Some P2P applications will also allow third parties to see the user's IP address. The installation of spyware is also common with many P2P applications.

Protecting the company's intellectual property

The use of P2P file-sharing applications can sometimes allow other members of the P2P network to have access to everything on a local machine, putting the company's intellectual property assets, as well as an employee's personal information, at risk.

806 Virtual Private Network (VPN) Policy

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Pinnacle Company Police and Pinnacle Security and Crime Prevention corporate network.

This policy applies to all Pinnacle Company Police and Pinnacle Security and Crime Prevention employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Pinnacle Company Police and Pinnacle Security and Crime Prevention network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Approved Pinnacle Company Police and Pinnacle Security and Crime Prevention employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Pinnacle Company Police and Pinnacle Security and Crime Prevention internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Pinnacle Company Police and Pinnacle Security and Crime Prevention network operational groups.
6. All computers connected to Pinnacle Company Police and Pinnacle Security and Crime Prevention internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from Pinnacle Company Police and Pinnacle Security and Crime Prevention's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Pinnacle Company Police and Pinnacle Security and Crime Prevention-owned equipment must configure the equipment to comply

with Pinnacle Company Police and Pinnacle Security and Crime Prevention's VPN and Network policies.

10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Pinnacle Company Police and Pinnacle Security and Crime Prevention's network, and as such are subject to the same rules and regulations that apply to Pinnacle Company Police and Pinnacle Security and Crime Prevention-owned equipment, i.e., their machines must be configured to comply with Pinnacle Company Police and Pinnacle Security and Crime Prevention's Security Policies.

807 Wireless Communication Policy

This policy prohibits access to Pinnacle Company Police and Pinnacle Security and Crime Prevention networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Pinnacle Company Police and Pinnacle Security and Crime Prevention are approved for connectivity to Pinnacle Company Police and Pinnacle Security and Crime Prevention's networks.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Pinnacle Company Police and Pinnacle Security and Crime Prevention's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Pinnacle Company Police and Pinnacle Security and Crime Prevention's networks do not fall under the purview of this policy.

807-A Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Pinnacle Company Police and Pinnacle Security and Crime Prevention. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with Pinnacle Company Police and Pinnacle Security and Crime Prevention.

807-B Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations.

807-C VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must

support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

807-D Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

808 Electronic Document Retention Policy

This policy applies to all employees who create electronic documents and all company, work-related, and personal documents stored on desktop/laptop machines, the company network, and personal digital assistants (PDAs).

The company has instituted this policy for the following reasons:

- To preserve storage space on the network and on users' laptops/desktops
- To encourage optimal performance of the company network
- To lessen the chance electronic documents could later be used in litigation against the company
- To eliminate confusion over different iterations of documents
- To ensure the authenticity of electronic documents on the network and the employees' laptops/desktops
- To ensure that important documents are not made unusable by technological upgrades

New employees will receive and sign this policy as part of the employee handbook.

Document types and guidelines

The following are the types of electronic documents and files covered under this policy. Other formats may be added as necessary.

1. **E-mail**—All e-mail—either from internal or external sources—is to be deleted after one year. Employees will strive to keep the majority of their e-mail related to business issues. Employees will receive automated notices from the IT department each month reminding them to delete old e-mail. In case the e-mail needs to be referenced or retrieved, the IT department will archive e-mail for six months after the employee has deleted it, after which time the e-mail will be permanently deleted. Employees will not store or transfer company-related e-mail on non-work-related computers. Employees will take care not to send confidential/proprietary company information to outside sources. Employees who have more than 100 MB in their e-mail account will be unable to send or receive messages until the size of their account is reduced. Any e-mail the employee deems vital to the performance of their job should be printed and stored in the employee's workspace.
2. **Web page files**—Employees will delete Web page files saved on the network or their local machines after one year. This includes pages saved from Web sites onto an employee's laptop/desktop.
3. **Text/formatted files**—Employees will conduct quarterly reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those

they consider unnecessary or outdated. After one year, all text files will be deleted from the network and the employee's desktop/laptop. Text/formatted files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.

4. **Sound and movie files**—Sound and movie files (e.g., MP3s, AVIs) used for business purposes will remain on the employee's desktop/laptop or network share indefinitely and will be deleted at the employee's discretion. Sound and movie files downloaded for personal use will be deleted after six months. Employees will adhere to the company's acceptable use policy when downloading sound and/or movie files for personal and/or business use.
5. **Spreadsheets**—As spreadsheets are often used with other departments (e.g., to determine revenue projections), please check with both your supervisor and your contact in the other department before deleting spreadsheets.
6. **PowerPoint presentations**—Because of their wide use within the company, employees will have the option of storing PowerPoint presentations on the network to encourage collaboration between various departments. All PowerPoint presentations should be deleted after one year.
7. **PDF documents**—After one year, employees will delete PDF files from their network shares and/or laptops and desktops.

Compliance

The company does not currently employ the means to automatically delete electronic files beyond the dates specified in this policy. Because of this, it is vital that employees adhere to the guidelines specified in this policy. Each quarter, IT will choose three employees at random and check their user shares on the network and their laptops/desktop to ensure they are in compliance. Files that are beyond the designated retention date will be deleted in accordance with this policy.

Exceptions

This policy does not apply to electronic documents related to litigation. IT will work closely with employees to ensure that the document retention guidelines are suspended for documents that have relevance to legal action. Employees who knowingly destroy documents related to civil or criminal litigation against the company will be immediately suspended pending an inquiry by the company's IT department. If it is found that the employee knowingly destroyed electronic documents related to litigation, the employee will be terminated and likely subject to civil and criminal penalties.

Revisions

Original – November 10, 2009

Employee Acknowledgment Form

The employee handbook describes important information about Pinnacle Company Police and Pinnacle Security and Crime Prevention. I understand that I should consult the Pinnacle Company Police and Pinnacle Security and Crime Prevention company manager regarding any questions not answered in the handbook. I have entered into my employment relationship with Pinnacle Company Police and Pinnacle Security and Crime Prevention voluntarily and acknowledge that there is no specified length of employment. Accordingly, either I or Pinnacle Company Police or Pinnacle Security and Crime Prevention can terminate the relationship at will, with or without cause, at any time.

Since the information, policies and benefits described here are necessarily subject to change, I acknowledge that revisions to the handbook may occur, except to Pinnacle Company Police and Pinnacle Security and Crime Prevention's policy of employment-at-will. All such changes will be communicated by appropriate notices, and I understand that revised information may supersede, modify, or eliminate existing policies. Only the Pinnacle Company Police and Pinnacle Security and Crime Prevention management has the ability to adopt any revisions to the policies in this handbook.

I have read and understand the policy/handbook that I have been issued.

Employee Printed Full Name

Employee Signature

Date

