



Employee Handbook

Rev. December 2022

Table of Contents

Welcome	4
About CyberFortress	4
Section 1: Employment At-Will	5
At-Will Employment	5
Section 2: Equal Employment Opportunity	5
Equal Opportunity Statement	5
Americans with Disabilities Act (ADA) & Reasonable Accommodations	5
Commitment to Diversity	6
Workplace Discrimination and Harassment	6
Sexual Harassment	6
Section 3: Terms of Employment.....	8
Employment Authorization Verification (I-9 Compliance).....	8
Classifications of Employment.....	8
Payroll and Employee Classification	8
Section 4: Employee Benefits	9
Health Insurance.....	9
Retirement Plan	10
Company Holidays.....	10
Vacation	10
Sick Leave	10
Section 5: Attendance & Leave	11
Attendance.....	11
Leave of Absence	11
Bereavement Leave.....	12
Military Leave (USERRA)	13
Jury and Witness Duty Leave.....	13
Time Off for Voting.....	13
Section 6: Employee Work, Hours & Pay	13
Work Schedules and Hours of Operation	13
Overtime	13
Meal and Rest Periods	14
Pay Period	14
Paycheck Deductions	14
Direct Deposit	14
Promotions & Transfers	14
Section 7: Workplace Conduct, Disciplinary Process & Best Practices	14
Standards of Conduct.....	14
Conflicts of Interest	15
Confidentiality	15
Employment of Relatives	15
Outside Employment	15
Dress Code Policy	15
Technology Systems	15
Computer Security and Copying of Software	16
Personal Cell Phone/Mobile Device Use.....	16
Social Media Guidelines	16
Section 9: Health and Safety	16
Commitment to Health & Safety	16
Workplace Security	16
Emergency Procedures	17
Drug and Alcohol Abuse Policy	17

Drug and Alcohol Testing	17
Smoke-Free Workplace	18
Workplace Violence	18
Workers' Compensation	19
Incident Reporting.....	19
Return to Work.....	19
Section 10: Personnel Records.....	20
Personal Data Changes	20
Personnel Records	20
Section 11: Separation of Employment.....	20
Resignation of Employment.....	20
Involuntary Separation.....	20
Final Paycheck	20
Exit Interview	20
Continuation of Benefits (COBRA)	20
Post-Employment Verification	20
State Addendum	21
Acknowledgment of Receipt and Review	22

Welcome

Welcome! You have just joined a dedicated organization. We hope that your employment with CyberFortress, LLC (“CyberFortress” or the “Company”) will be rewarding and challenging. We take pride in our employees as well as in the products and services we provide.

CyberFortress complies with federal law and all applicable state and local employment laws.

Please take the time now to read this handbook carefully. Sign the acknowledgement at the end to show that you have received and understand this handbook, which sets out the basic rules and guidelines concerning your employment. This handbook supersedes any previously issued handbooks or policy statements dealing with the subjects discussed herein. CyberFortress reserves the right to interpret, modify, or supplement the provisions of this handbook at any time. Neither this handbook nor any other communication by a management representative or other, whether oral or written, creates or is intended in any way to create a contract of employment. Please understand that no employee handbook can address every situation in the workplace. You are encouraged to reach out to your manager or Human Resources with questions.

If you have questions about your employment or any provisions in this handbook, contact your manager, or Human Resources.

We wish you success in your employment here at CyberFortress!

About CyberFortress

As an organization, our purpose is to build a company that maximizes the potential in ourselves and others. As a team, we take pride in the following Core Values:

- **People First:** We provide the opportunity for everyone to do meaningful work with people they love to work with.
- **Humble and Driven to Results:** We “roll up our sleeves” and are willing to pitch in when and where it is needed.
- **Why and What's Next:** We let curiosity continue to ask the next question until we have a clear picture of a great outcome.
- **Act on the Truth:** We speak up, get to the facts of the situation, and make the hard decisions in a healthy way.

We also take pride in providing an excellent and personalized service experience around digital record protection for our customers.

We look forward to continuing to build our culture around the collective knowledge, ideas, and experiences of our combined team.

Section 1: Employment At-Will

At-Will Employment

Your employment with CyberFortress is on an "at-will" basis. This means your employment may be terminated at any time, with or without notice and with or without cause. Likewise, we respect your right to leave CyberFortress at any time, with or without notice and with or without cause.

Nothing in this handbook or any other Company document should be understood as creating a contract, guaranteed or continued employment, a right to termination only "for cause," or any other guarantee of continued benefits or employment. Only the Chief Executive Officer has the authority to make promises or negotiate with regard to guaranteed or continued employment, and any such promises are only effective if placed in writing and signed by the Chief Executive Officer.

If a written contract between you and CyberFortress is inconsistent with this handbook, the written contract is controlling.

Nothing in this handbook will be interpreted, applied, or enforced to interfere with, restrain, or coerce employees in the exercise of their rights under Section 7 of the National Labor Relations Act.

Section 2: Equal Employment Opportunity

Equal Opportunity Statement

CyberFortress is committed to the principles of equal employment opportunity. We are committed to complying with all federal, state, and local laws providing equal employment opportunities, and all other applicable employment laws and regulations. We are committed to maintaining a work environment that is free of harassment, discrimination, or retaliation because of sex (including pregnancy, childbirth, breastfeeding and/or related medical conditions), gender, gender expression, gender identity, race, religion, color, national origin, disability, genetic information, marital status, age, sexual orientation, AIDS/HIV status, military service, veteran status, or any other status protected by federal, state, or local laws. CyberFortress is dedicated to the fulfillment of this policy regarding all aspects of an applicant's or employee's relationship with CyberFortress, including but not limited to recruiting, hiring, transfer, training, promotion, rates of pay, and termination.

CyberFortress will conduct a prompt and thorough investigation of all allegations of discrimination, harassment, retaliation, or any violation of the Equal Employment Opportunity Policy. CyberFortress will take appropriate corrective action, if and where warranted. CyberFortress prohibits retaliation against employees who provide information about, complain about, or assist in the investigation of any complaint of discrimination or violation of the Code of Conduct and Business Ethics. We are all responsible for upholding this policy. You may discuss questions regarding equal employment opportunities with your manager or any other designated member of management.

Americans with Disabilities Act (ADA) & Reasonable Accommodations

CyberFortress complies with the Americans with Disabilities Act (ADA), the Pregnancy Discrimination Act, and all applicable state and local fair employment practices laws and is committed to providing equal employment opportunities to qualified individuals with disabilities, including disabilities related to pregnancy, childbirth, and related conditions.

Consistent with this commitment, CyberFortress will provide reasonable accommodation to otherwise qualified individuals where appropriate to allow the individual to perform the essential functions of the job, unless doing so would create an undue hardship on the business.

If you require an accommodation because of your disability, it is your responsibility to notify your manager or HR Department. You may be asked to include relevant information such as:

- A description of the proposed accommodation
- The reason you need an accommodation
- How the accommodation will help you perform the essential functions of your job
- Medical certification that substantiates the needs of an accommodation

After receiving your request, CyberFortress will engage in an interactive process with you to determine the nature of the issue and what, if any, reasonable accommodation(s) may be appropriate. Where appropriate, we may need your permission to obtain additional information from your medical provider. All medical information received by CyberFortress in connection with a request for accommodation will be treated as confidential.

CyberFortress encourages you to suggest specific reasonable accommodations that you believe would allow you to perform your job. However, CyberFortress is not required to make the specific accommodations requested by you and may provide an alternative accommodation, to the extent any reasonable accommodation can be made without imposing an undue hardship on CyberFortress.

If leave is provided as a reasonable accommodation, such leave may run concurrently with leave under the federal Family and Medical Leave Act and/or any other leave where permitted by state and federal law.

CyberFortress will not discriminate or retaliate against employees for requesting an accommodation.

Commitment to Diversity

CyberFortress is committed to creating and maintaining a workplace in which all employees have an opportunity to participate and contribute to the success of the business and are valued for their skills, experience, and unique perspectives. This commitment is embodied in company policy and the way we conduct business at CyberFortress and is an important principle of sound business at CyberFortress.

Workplace Discrimination and Harassment

Having a diverse workforce--made up of team members who bring a wide variety of skills, abilities, experiences, and perspectives are essential to CyberFortress' success. The Company is committed to the principles of equal employment opportunity, inclusion, and respect. CyberFortress does not tolerate discrimination against anyone--team members, customers, business partners, or other stakeholders—on the basis of race, color, religion, national origin, sex (including pregnancy), age, disability, sexual orientation, gender identity, marital status, past or present military service, or any other status protected by the laws or regulations in the locations where CyberFortress operates. CyberFortress complies with laws regarding employment of immigrants and non-citizens and provides equal employment opportunity to everyone who is legally authorized to work in the applicable country. CyberFortress provides reasonable accommodations to individuals with disabilities and removes any artificial barriers to success.

As is the case with any violation of the Code, all CyberFortress employees and representatives have a responsibility to report any discriminating or harassing behavior or condition even if they are not directly involved or are just a witness. Retaliation for making a complaint or for assisting in the investigation of discrimination or harassment complaint is prohibited.

Sexual Harassment

Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature.

While it is not possible to identify every act that constitutes or may constitute sexual harassment, the following are some examples of sexual harassment:

- Unwelcome requests for sexual favors
- Lewd or derogatory comments or jokes
- Comments regarding sexual behavior or the body of another
- Sexual innuendos and other vocal activity such as catcalls or whistles
- Obscene letters, notes, emails, invitations, photographs, cartoons, articles, or other written or pictorial materials of a sexual nature
- Repeated requests for dates after being informed that interest is unwelcomed
- Retaliating against another for refusing a sexual advance or reporting an incident of possible sexual harassment to CyberFortress or any government agency
- Offering or providing favors or employment benefits such as promotions, favorable evaluations, favorable assigned duties, or shifts, etc., in exchange for sexual favors; and

- Any unwanted physical touching or assaults or blocking or impeding movements.
- Hostile work environment

Other Prohibited Harassment

Other workplace harassment includes any verbal or physical conduct that insults or shows hostility or aversion towards an individual because of the individual's gender, race, religion, color, national origin, disability, genetic information, marital status, age, sexual orientation, AIDS/HIV status, military service, veteran status, or any other status protected by federal, state, or local laws.

Again, while it is not possible to list all the circumstances that may constitute other forms of workplace harassment, the following are some examples of conduct that may constitute workplace harassment:

- The use of disparaging or abusive words or phrases, slurs, negative stereotyping, or threatening, intimidating, or hostile acts that relate to the above protected categories
- Written or graphic material that insults, stereotypes, or shows aversion or hostility towards an individual or group because of one of the above protected categories and that is placed on walls, bulletin boards, email, voicemail, or elsewhere on our premises, or circulated in the workplace; and
- A display of symbols, slogans, or items that are associated with hate or intolerance toward an individual's protected status.

Reporting Discrimination and Harassment

If you believe you are being subjected to any of the behaviors described above, report the concerning conduct immediately to one of the following report persons: (1) any officer of CyberFortress; (2) any member of Human Resources, or our Chief Ethics and Compliance Officer.

Do not assume that CyberFortress is already aware of your situation. Even if members of management observe the conduct, they may not know that the conduct or comments are offensive to you. What is funny to one person may be offensive to another. A hug may be welcomed by one person and make another person very ill at ease. Bystanders are often unaware of the impact of the conduct on any individual. Therefore, it is your responsibility to bring your concerns to CyberFortress' attention by following the reporting procedure outlined above so that we can help resolve them.

If the person engaging in the harassing behavior is one of the persons listed above as a report person, simply telling the person to stop the harassing behavior will not serve as a report of your concern because that individual may fail to report their own conduct. Then the problem may never be brought to the attention of Human Resources to be properly addressed. Therefore, in this situation, you must report the conduct to an officer of CyberFortress or any member of Human Resources other than the person engaging in the harassing behavior.

Investigation of Unwelcome Harassment

Reports by employees that they believe they have been subjected to unwelcome harassment will be treated seriously, and where the report is of conduct that would be a violation of this policy, an investigation will be initiated promptly unless the circumstances surrounding the conduct giving rise to the complaint are not in dispute. To the extent that it is reasonably practicable, CyberFortress will maintain confidentiality. All employees are required to cooperate in a Company investigation.

Disciplinary Measures

Where an investigation reveals that allegations of unwelcome harassment are true, appropriate remedial action, including discipline, will be taken. All disciplinary measures will be implemented promptly and shall be commensurate with the person's conduct. The remedies vary depending on the entire facts and circumstances found by the investigation, and employees who have been found to have engaged in inappropriate conduct that does not rise to the level of harassment may nevertheless be disciplined. If the investigation reveals that the charges were brought falsely and with malicious intent, the charging party may be subject to disciplinary action, up to and including termination.

Harassment By Customers and Vendors

CyberFortress recognizes that unwelcome harassment can also be perpetrated by a customer, vendor, or employee of a vendor of CyberFortress. Should this occur, the reporting and investigation procedures discussed above will

be followed. Where the investigation reveals that allegations of unwelcome harassment are true, CyberFortress will undertake appropriate measures to ensure that the harassment stops.

Section 3: Terms of Employment

Employment Authorization Verification (I-9 Compliance)

All offers of employment are contingent on verification of your right to work in the United States. New hires will be required to complete Section 1 of federal Form I-9 on the first day of paid employment and must present acceptable documents authorized by the U.S. Citizenship and Immigration Services proving identity and employment authorization no later than the third business day following the start of employment with CyberFortress. If you at any time cannot verify your right to work in the United States, CyberFortress may be obligated to terminate your employment.

If you are authorized to work in this country for a limited period of time, you will be required to submit proof of renewed employment eligibility prior to expiration of that period to remain employed by CyberFortress.

Classifications of Employment

Employees are placed into several different classifications for the administration of compensation and benefits.

Full-time employees are those who are normally scheduled to work and who do work a schedule of at least 30 hours per week.

Part-time employees are those who are normally scheduled to work and who do work less than 30 hours per week.

Non-exempt employees, as defined by either the Federal Fair Labor Standards Act or applicable state law, are those who are generally required to be paid overtime for all hours worked more than forty during a one-week work period. In other words, they are not exempt from overtime. Some state or local laws may require overtime based upon hours worked in a day, rather than in a week.

Salaried non-exempt employees are those who are paid on a salary basis, work a fixed number of hours and are still eligible to receive overtime compensation.

Exempt employees are employees who work in positions that are excluded from overtime pay requirements under applicable state and federal law. Compensation, paid as salary, pays for all hours worked. Most exempt employees are paid a salary.

Contract employees are also called leased employees, independent contractors, contract workers, freelancers, or work-for-hire staffers, are individuals hired for a specific project or a certain time frame for a set fee. Often, contract employees are hired due to their expertise in a particular area.

If you have any questions about your employment classification, please contact your manager or the Human Resources department.

Payroll and Employee Classification

It is CyberFortress' policy and practice to accurately compensate employees and to do so in compliance with all applicable state and federal laws. To ensure proper payment for all time worked and all proper deductions have been made, employees must correctly record their work time and review each paycheck to identify and report any errors. Off-the-clock or unrecorded work is not allowed.

Review Your Pay Stub. We make every effort to ensure our employees are paid correctly. An occasional inadvertent mistake can happen. If so, please bring errors to our attention and prompt corrections will be made. Please review your pay stub when you receive it. If you believe a mistake has occurred or if you have any questions, please use the reporting procedure outlined below.

Non-exempt Employees. Employees eligible for overtime pay or extra pay must maintain a record of the total hours worked each day. These hours must be accurately recorded on a timekeeping system provided to employees. Each employee must approve his or her timecard to verify that the reported hours worked are complete and accurate (and that there is no unrecorded or “off-the-clock” work). Timecards must accurately reflect all regular and overtime hours worked, any absences, early or late arrivals, early or late departures and meal breaks. At the end of each pay period, completed timecards should be submitted for verification and approval. When you receive a paycheck, please verify immediately that you were paid correctly for all regular and overtime hours worked each workweek.

Exempt Employees. Exempt salaried employees receive a salary which is intended to compensate you for all hours worked for CyberFortress. This salary will be established at the time of hire or when an exempt employee classification is made. While such salary may be subject to modification from time to time, such as during salary review times, the salary will be a predetermined amount that will not be subject to deductions for variations in the quantity or quality of the work you perform.

Exempt employees will receive their full salary for any workweek in which work is performed.

Exempt employees' salaries may be reduced for certain types of deductions, such as: the employee's portion of health, dental or life insurance premiums; state, federal or local taxes, social security; or voluntary contributions to a 401(k) or pension plan.

Please note: Exempt employees may be required to use vacation, PTO, personal days, or other forms of paid time off for full or partial day absences for personal reasons, sickness, or disability. However, such salary will not be reduced for partial day absences if the exempt employee does not have accrued paid time off.

To Report Violations of This Policy, Communicate Concerns, or Obtain More Information

It is a violation of CyberFortress' policy for any employee to falsify a timecard, or to alter another employee's timecard. It is also a serious violation of Company policy for any employee or manager to instruct another employee to incorrectly or falsely report hours worked or alter another employee's timecard to either under or over report hours worked. If any manager or employee instructs you to (1) incorrectly or falsely under or over report your hours worked, (2) alter another employee's time records to inaccurately or falsely report that employee's hours worked, or (3) conceal any falsification of time records or to violate this policy, do not do so. Instead, report it immediately to your manager or the Chief Ethics and Compliance Officer.

Employees should not work any hours outside of the scheduled workday unless authorized by a manager in advance. Employees should not start work early, finish work late, work during a meal break or perform any other extra or overtime work unless authorized to do so and that time is recorded on a timecard. Employees are prohibited from performing any “off-the-clock” work. “Off-the-clock” work means work you may perform but fail to report on your timecard. Any employee who fails to report or inaccurately reports any hours worked will be subject to disciplinary action, up to and including termination.

If you have questions about deductions from your pay, please contact your manager immediately. If you believe your wages have been subject to any improper deductions or your pay does not accurately reflect all hours worked, you should report your concerns to a manager immediately. If a manager is unavailable or if you believe it would be inappropriate to contact that person or if you have not received a prompt and fully acceptable reply, you should immediately contact Human Resources.

Section 4: Employee Benefits

Health Insurance

CyberFortress makes group health benefits available to full-time employees and their family members. If elected, the health insurance is effective on the first day of employment. Health benefits are paid in part by CyberFortress. The remainder of the costs is the employee's responsibility. Employees will receive details about benefits provided, contribution rates and eligibility upon new hire onboarding.

Retirement Plan

CyberFortress participates in a 401(k) plan so that employees may save a portion of their earnings for retirement. Regular employees who have worked at least thirty hours per week are eligible. Employees may elect to make regular contributions to the 401(k) plan up to the maximum amount allowed by federal law.

Contact Human Resources for detailed information regarding eligibility, employee contributions, vesting period or employer contributions. More information can also be found in the plan summary description, which is available from the employee portal.

If there are any inconsistencies between this handbook and any of the Summary Plan Descriptions, the Summary Plan Descriptions shall govern.

Company Holidays

CyberFortress observes the following holidays:

- New Year's Day
- Martin Luther King, Jr. Day
- George Washington's Birthday (commonly known as President's Day)
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veterans Day
- Thanksgiving
- Christmas Day

Full-time employees are eligible for paid holiday benefits. Further details regarding paid holidays are included in the benefits booklet.

Vacation

CyberFortress provides paid vacation benefits to full-time and part-time employees. Eligible employees are front loaded vacation based on an employee's classification, upon their hire date as well as the beginning of each calendar year. At year end, you are allowed to carryover 1 week (40 hours) of vacation hours.

Employees should request to schedule vacation time off as far in advance as possible electronically, through the timekeeping system. Vacations will be scheduled to provide adequate coverage of jobs and staff requirements. CyberFortress will make the final determination in this regard.

Vacation pay is not counted for the purpose of calculating an employee's overtime hours of work or overtime premiums.

Vacation benefits are not accrued, as such, unused vacation benefits will not be paid upon termination of employment unless state law requires otherwise.

Sick Leave

CyberFortress offers paid sick leave to regular full-time employees who are hired between January and September at the rate of 7 days per year. Employees hired after 1 October will receive 3 days. Sick leave is to be used only when an employee needs to recover from illness or injury, or to attend medical and dental appointments, unless otherwise required by applicable state law. CyberFortress will not tolerate abuse or misuse of sick leave.

An employee who is unable to report to work because of injury or illness must notify their supervisor prior to the scheduled starting time and should refer to the Attendance section of the Handbook for specific requirements for calling in sick.

CyberFortress reserves the right to require a release from the employee's health care provider before the employee returns to work.

Sick leave does not carry over from year to year unless required by state or local law. Moreover, employees are not compensated for unused sick leave at the end of employment with CyberFortress or at any other time.

For employees working in a jurisdiction that has a mandatory sick leave law or a jurisdiction that defines how sick leave may be used or accrued, CyberFortress will comply with all legal requirements, including providing greater or different benefits than those indicated here. In such a situation, the leave the employee is entitled to under the law may run concurrently with the leave provided under this policy, to the extent permissible under applicable law.

Section 5: Attendance & Leave

Attendance

CyberFortress has operations running 24 hours per day, every day of the year, to support the operations of the services we provide to our customers. Work hours will vary depending on work location and job responsibilities. Supervisors will provide employees with their work schedule. Should an employee have any questions regarding his/her work schedule, the employee should contact their manager. You must give reasonable notice of your absence or tardiness for CyberFortress to manage its business obligations. You are required to call your manager at least one (1) hour before the start of your work schedule. If you could not reasonably foresee your need for leave, you must call or email your manager about the anticipated absence or tardiness as soon as possible.

Repeated absenteeism, tardiness, or failure to call in each day of absence will be cause for disciplinary action, including termination. If you are experiencing an issue that is causing you to be late for work and/or are unable to attend work as regularly scheduled, it is your responsibility to immediately notify your manager to discuss the situation prior to being tardy or absent. CyberFortress will evaluate each situation in accordance with all applicable laws and regulations.

Job Abandonment

If you fail to show up for work or call in with an acceptable reason for the absence for a period of three (3) consecutive days, you will be considered to have abandoned your job and voluntarily terminated your employment with CyberFortress.

Leave of Absence

Personal Leave

Requests for personal leave will be considered and evaluated on an individual basis. Unpaid leave may be granted for up to 30 days for full-time employees who have completed at least 6 months of service.

Approval or denial of such requests will be entirely at CyberFortress' discretion. In determining the feasibility of granting such requests, factors such as the purpose of requested leave, availability of coverage for job responsibility during the requested leave, previous absences, length of employment, prior work records and performance and similar considerations, will be considered. Such requests must be submitted to the Human Resources department, after they have received written approval from their department leader.

Employees on leave are asked to confirm their return date at least two weeks before they return to work. Any requests for additional leave must be made as soon as possible. Employees on leave who do not return as scheduled and fail to request or cannot show a good reason why an extension should be granted, will be considered to have voluntarily terminated their employment as of the day the original leave expired.

Paid Parental Leave

Active full-time and part-time employees, who have completed 6 months of continuous employment, are eligible for CyberFortress' Paid Parental Leave. Short-term, temporary and interns are not eligible for paid family leave. Paid Parental Leave will run concurrently with federal and/or state leave.

Eligibility

An eligible employee shall be entitled to take up to twelve (12) weeks of paid and job protected leave in a twelve (12) month rolling period for the birth parent, and four (4) weeks for the non-birth parent for any of the following reasons:

- Have given birth to a child
- Birth of a child through a surrogacy
- Be a spouse or partner of a birth parent
- Have adopted a child (the child must be age 18 or younger)
- Must be the intended parent of the child

Notice of Leave

If you need one of the listed leaves, you must give CyberFortress at least a 30 days' notice. If the leave is not foreseeable, provide as much prior notice as soon as practicable (within one to two business days of learning of your need for leave). Failure to provide such notice may be grounds for delaying covered leave, depending on the particular facts and circumstances.

Contact Human Resources to request leave and complete the leave of absence form.

Certification of Need for Leave

If an employee requests one of the listed leaves based upon his/her own serious health condition, or the serious health condition of a spouse, child, or parent, CyberFortress may require, in its discretion, that the employee submit a medical certification, in a form approved by CyberFortress, which must be completed by the employee's or family member's health care provider, as appropriate, regarding the serious health condition.

When you request leave, CyberFortress will notify you of the requirement for medical certification and when it is due (at least 15 days after you request leave). Failure to provide requested medical certification in a timely manner may result in denial of leave until it is provided.

In addition, CyberFortress will require employees to submit periodic recertifications of the serious health condition. Any medical certification must be returned by the employee within 15 days or CyberFortress may delay the commencement or continuation of the leave until the certification is submitted.

CyberFortress also reserves the right to require certification from a covered military member's health care provider if you are requesting military caregiver leave and certification in connection with military exigency leave.

Reporting While on Leave

If you take leave because of your own serious health condition or to care for a covered relation, you must contact CyberFortress every thirty (30) days regarding the status of the condition and your intention to return to work. In addition, you must give notice as soon as practicable (within two business days if feasible) if the dates of leave change or are extended or initially were unknown.

Medical and Other Benefits

During approved leave, CyberFortress will maintain your health benefits as if you continued to be actively employed.

Returning From Leave; Restoration to Employment

If you take leave because of your own serious health condition (except if you are taking intermittent leave), you are required, as are all employees returning from other types of medical leave, to provide medical certification that you are fit to resume work. Otherwise, you will not be permitted to resume work until it is provided.

An employee who takes family or medical leave in accordance with this policy shall have the right to return to the position he/she held prior to the leave or, to an equivalent position with the same pay, benefits, and terms and conditions of employment. Please refer to the Paid Leave Policy if you have any questions.

Bereavement Leave

Employees may take up to three (3) days of paid time off to attend the funeral and make any necessary arrangements due to the death of an immediate family member, except where allowed additional time off for bereavement under applicable state law. "Immediate family" consists of the employee's spouse, domestic partner, child, sibling, parents, grandparents, grandchildren, or the child, sibling or parents of the employee's spouse or domestic partner.

Employees must notify their supervisor as soon as possible if they need to take bereavement leave. Approval of bereavement leave will occur in the absence of unusual CyberFortress operating requirements. Any employee may,

with their supervisor's approval, use any available vacation benefit for additional time off beyond three days as necessary.

Military Leave (USERRA)

A military leave of absence will be granted to employees who are absent from work because of service in the U.S. uniformed services, in accordance with the Uniformed Services Employment and Reemployment Rights Act (USERRA) and applicable Company policy. Advance notice of military service is required, unless military necessity prevents such notice, or it is otherwise impossible or unreasonable. Employees are required to give or send written details of any United States military commitments to Human Resources. Duty orders must be submitted immediately to Human Resources upon receipt from the military. Laws governing the rights of employees taking military leave are frequently amended and Human Resources should be consulted to ensure that the most current rights are properly honored and observed by CyberFortress.

Continuation of health insurance benefits is available as required by USERRA based on the length of the leave and subject to the terms, conditions, and limitations of the applicable plans for which the employee is otherwise eligible.

Employees on military leave for up to 30 days are required to return to work for the first regularly scheduled shift after the end of service, allowing reasonable travel time. Employees on military leave between 31 and 180 days have 14 days from the end of their service to report back to work. Those employees who serve more than 180 days must return to work within 90 days of the end of their military service. Employees on military leave longer than 30 days must apply for reinstatement in accordance with USERRA and all applicable state laws.

Employees returning from military leave will be placed in the position they would have attained had they remained continuously employed or a comparable one depending on the length of military service in accordance with USERRA, and benefits will be reinstated as required by the laws in effect at the time of return.

Laws regarding military leaves of absence change frequently. If you would like further information concerning military leaves of absence and your rights under current laws, please contact Human Resources.

Jury and Witness Duty Leave

We encourage employees to serve on jury or witness duty when called. Employees must notify their supervisor of the need for time off for jury or witness duty upon receipt of a subpoena, notice or summons from the court. CyberFortress will compensate employees for the difference between jury duty compensation and your current daily pay for the first five (5) days you serve as a juror (or in accordance with applicable law, if different). If additional time is required, it will be granted, but without pay.

Employees may be required to provide verification of jury duty or witness service from the court clerk. Employees on jury or witness duty are expected to report or return to work for the remainder of the work schedule when dismissed from jury or witness duty.

Time Off for Voting

CyberFortress encourages all employees to vote. Most polling facilities for elections for public office are scheduled to accommodate working voters. CyberFortress, therefore, requests that employees schedule their voting for before or after their work shift. An employee who expects a conflict should notify his or her manager, in advance, so that schedules can be adjusted if necessary.

Section 6: Employee Work, Hours & Pay

Work Schedules and Hours of Operation

Hours and work schedules may vary according to business needs and position. Your manager will assign you to your individual work schedule. Employees should contact their direct manager for their scheduling requests.

Overtime

When operating requirements or other needs cannot be met during regular working hours, employees may be scheduled to work overtime. We will attempt to give as much notice as possible in this instance. However, advance notice may not always be possible. Nonexempt employees will be paid one and one-half (1.5) times their regular

rate of pay for all hours worked more than 40 in one workweek and as otherwise required by applicable state and federal law. Paid time off such as sick pay, holiday pay, vacation pay, bereavement pay, and jury duty pay (where applicable) will not count toward hours worked for the purpose of determining overtime pay.

All overtime work must be authorized in advance by the employee's manager, in writing. Working overtime without prior authorization may result in disciplinary action.

Exempt employees are expected to work as much of each workday as is necessary to complete their job responsibilities. No overtime or additional compensation is provided to exempt employees.

Meal and Rest Periods

CyberFortress strives to provide a safe and healthy work environment and complies with all applicable laws regarding meal and rest periods. Check with your manager regarding procedures and schedules for rest and meal breaks.

Pay Period

The standard pay period is semi-monthly for all employees unless applicable law requires more frequent payment. Standard pay dates are the 7th and 22nd of the month. If a pay date falls on a holiday or the weekend, you will be paid on the preceding workday.

Review your paycheck for accuracy. If you find an issue, report it to your manager immediately.

Paycheck Deductions

CyberFortress is required by law to make certain deductions from your pay each pay period. This includes income and any unemployment taxes, Federal Insurance Contributions Act (FICA) contributions, Social Security and Medicare, and any other deductions required under law or by court order for wage garnishments. The amount of your tax deductions will depend on your earnings and the number of exemptions you list on your federal Form W-4 and applicable state withholding form. You may also authorize voluntary deductions from your paycheck, including contributions for insurance premiums, retirement plans, spending accounts, or other services. Your deductions will be reflected in your wage statement.

CyberFortress will not make deductions to your pay that are prohibited by federal, state, or local law. If you have any questions about deductions from your pay or believe you have been subjected to improper deductions, promptly contact your payroll specialist. Every report will be fully investigated, and CyberFortress will provide the employee with any compensation to which the employee is entitled in a timely fashion.

Direct Deposit

CyberFortress encourages all employees to enroll in direct deposit. If you would like to take advantage of direct deposit, you can set that up in your Human Resources portal.

If you have selected the direct deposit payroll service, you will receive electronic confirmation of all deductions.

Promotions & Transfers

It is our policy to promote from within only when the most qualified candidate is available. Promotions are made on an equal opportunity basis according to employees possessing the needed skills, education, experience, and other qualifications that are required for the job.

Section 7: Workplace Conduct, Disciplinary Process & Best Practices

Standards of Conduct

CyberFortress wishes to create a work environment that promotes job satisfaction, respect, responsibility, integrity, and value for all our employees, clients, customers, and other stakeholders. We all share the responsibility of improving the quality of our work environment. For additional information, refer to our Code of Conduct.

Conflicts of Interest

CyberFortress is concerned with conflicts of interest that create actual or potential job-related concerns, especially in the areas of confidentiality, customer relations, safety, security, and morale. If there is any actual or potential conflict of interest between you and a competitor, supplier, distributor, or contractor to CyberFortress, you must disclose it to the Chief Ethics and Compliance Officer. If an actual or potential conflict of interest is determined to exist, CyberFortress will take such steps as it deems necessary to reduce or eliminate this conflict.

Confidentiality

As a condition of employment, CyberFortress employees must execute an Employee Proprietary Information Agreement upon beginning employment with CyberFortress. Each employee is responsible for safeguarding confidential information obtained in connection with his or her employment. In the course of your work, you may have access to confidential information regarding CyberFortress, its suppliers, its customers, or perhaps even fellow employees. It is your responsibility to in no way reveal or divulge any such information unless it is necessary for you to do so in the performance of your duties. Access to confidential information should be on a “need-to-know” basis and must be authorized by your manager. Your obligations to maintain the confidentiality of this information will continue after your employment with CyberFortress terminates. Any breach of this policy will not be tolerated, and legal action may be taken by CyberFortress.

Please note that nothing in this Employee Handbook is intended to affect an employee’s right to discuss the terms, wages, and working conditions of his/her employment, as protected by applicable law.

Employment of Relatives

We will not employ friends or relatives in circumstances where actual or potential conflicts may arise that could compromise supervision, safety, confidentiality, security, and morale at CyberFortress. It is your obligation to inform CyberFortress of any such potential conflict so the CyberFortress can determine how best to respond to the situation.

Outside Employment

Outside employment that creates a conflict of interest or that affects the quality or value of your work performance or availability at CyberFortress is prohibited. CyberFortress recognizes that you may seek additional employment during off hours, but in all cases expects that any outside employment will not affect job performance, work hours, or scheduling, or otherwise adversely affect your ability to effectively perform your duties. Any conflicts should be disclosed to the Chief Ethics and Compliance Officer. Failure to adhere to this policy may result in discipline up to and including termination.

Dress Code Policy

We trust employees to dress appropriately. Comfort is fine but consider what customers and other employees will think. Your department may have some specific requirements, so check with your manager. If you are wearing something inappropriate, you will receive feedback.

Technology Systems

CyberFortress provides an email system, voicemail system, access to the Internet, and other technology systems to assist employees in conducting Company business. All information, data, and messages created, received, sent, or stored in these systems are, at all times, the property of CyberFortress. All existing Company policies apply to Employee conduct on the Internet and use of all technology systems, including, but not limited to, Company policies regarding intellectual property, misuse of Company property, discrimination, harassment, sexual harassment, information and data security, and confidentiality.

Non-Business Use

CyberFortress wishes to foster an environment of open communications where employees enjoy their work. CyberFortress recognizes that employees spend a significant portion of their day at work and there will be occasions when it will be reasonable or even necessary to use CyberFortress’ technology systems for personal and non-work communications. To that end, CyberFortress does not prohibit usage of its technology systems for the purpose of communications that are unrelated to work, provided that such usage is (i) limited, (ii) does not interfere with work performance or business needs, and (iii) is in compliance with Company policies and management directives.

Unauthorized Access

Employees may access only files or programs, whether computerized or not, that they have permission to access or possess. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems or programs, or other property of CyberFortress, or improper use of information obtained by unauthorized means, may be grounds for disciplinary action, up to and including termination.

Computer Security and Copying of Software

Software programs purchased and provided by CyberFortress are to be used only for creating, researching, and processing materials for Company use. By using Company hardware, software, and networking systems you assume personal responsibility for their use and agree to comply with this policy and other applicable Company policies, as well as city, state, and federal laws and regulations.

All software acquired for or on behalf of CyberFortress or developed by Company employees or contract personnel on behalf of CyberFortress, is and will be deemed Company property. It is the policy of CyberFortress to respect all computer software rights and to adhere to the terms of all software licenses to which CyberFortress is a party.

You may not illegally duplicate any licensed software or related documentation. Unauthorized duplication of software may subject you and/or CyberFortress to both civil and criminal penalties under the United States Copyright Act. To purchase software, obtain your manager's approval.

You may not duplicate, copy, or give software to any outsiders including clients, contractors, customers, and others. You may use software on local area networks or on multiple machines only in accordance with applicable license agreements entered into by CyberFortress.

Prohibited Uses

CyberFortress does not allow its technology systems to be used in creating, receiving, sending, or storing data that may reasonably be offensive, defamatory, obscene, or harassing. Such data includes, but is not limited to, sexual images and comments, racial and gender-based slurs, or anything that would reasonably be expected to offend someone based on their disability, age, religion, marital status, sexual orientation, national origin, or culture, or any other factor protected by law. Any such use would violate this policy and may violate CyberFortress' Policy Prohibiting Discrimination, Harassment, and Retaliation. In particular, the display of any kind of sexually explicit image or document on any Company system is a violation of CyberFortress' policy. Employees who are aware of the misuse of these systems by other employees shall report the misuse to a manager immediately.

Personal Cell Phone/Mobile Device Use

While CyberFortress permits employees to bring personal cell phones and other mobile devices (i.e., smart phones, PDAs, tablets, laptops) into the workplace, you must not allow the use of such devices to interfere with your job duties or impact workplace safety and health.

Social Media Guidelines

To minimize risks to CyberFortress, you are expected to follow our Social Media guidelines covered in our Code of Conduct.

Section 9: Health and Safety

Commitment to Health & Safety

It is the responsibility of all CyberFortress employees to maintain a healthy and safe work environment. Report all safety hazards and occupational illnesses or injuries to your manager as soon as reasonably possible and complete an occupational illness or injury form as needed. Failure to follow CyberFortress health and safety rules may result in disciplinary action, up to and including termination of employment.

Workplace Security

Employees must be alert and aware of any potential dangers to themselves or their coworkers. Take every precaution to ensure that your surroundings are safe and secure. Guard personal belongings and Company property. Visitors should always be escorted. Report any suspicious activity to a manager immediately.

Emergency Procedures

In the event of an emergency, dial 911 immediately. If you hear a fire alarm or other emergency alert system, proceed quickly and calmly to the nearest exit. Once the building has been evacuated, only a manager may authorize employees to reenter.

Drug and Alcohol Abuse Policy

CyberFortress wants a drug and alcohol-free work environment, so we prohibit the use, possession, sale, or solicitation of certain prohibited substances at the workplace by employees. "Prohibited substances" include alcohol, illegal drugs, prescription drugs taken without a prescription or not taken in accordance with the prescription, or synthetic substitutes for those substances.

Prohibited activities include, but are not limited to, the following:

- The actual or attempted use, possession, manufacture, distribution, solicitation, or sale of illegal drugs while working or on duty (including during lunch and other breaks), while using Company assets or on Company property, or on Company business
- Bringing any form of illegal drug (including drug paraphernalia) onto any Company property or any other premises where employees are assigned or to which they travel as a part of their job duties
- Testing positive for alcohol while working, including during lunch and other breaks
- Being under the influence of illegal drugs while working (including during lunch and other breaks), while using Company assets or on Company property, or on Company business. Additionally, the possession or use of illegal drugs off-duty will not be tolerated to the extent such possession or use results in the employee's reporting to work or presence on Company property under the influence of illegal drugs
- Refusal to comply with drug testing, testing schedules and instructions, or diluting or otherwise attempting to alter or altering a specimen for drug testing
- Refusal to submit to a lawful Company-requested search
- Testing positive for illegal drugs, e.g., testing positive for a detectable level of any illegal drug
- The unauthorized use or being under the influence of alcohol while working or on duty (including during lunch and other breaks), while using Company assets or on Company property, or on Company business. Additionally, the possession or use of alcohol when off-duty will not be tolerated to the extent such possession or use results in the employee's reporting to work or presence on Company property while under the influence of alcohol. At Company sponsored special events as well as in those situations where employees are engaged in business travel or entertainment or business-related social events where alcohol is being served, the employee is expected to regulate his/her alcohol consumption and that of his/her guest(s) so as not to become impaired
- The unauthorized possession of alcohol, including having open containers, while at work, on Company property, in Company vehicles, rental vehicles, or personal vehicles while being used for Company business
- Not complying with alcohol-related rehabilitation requirements

Drug and Alcohol Testing

Where permitted by applicable state law, an employee may be required to undergo a blood test, urinalysis, "breath-analyzer" test or other diagnostic test under the following circumstances:

1. Reasonable Cause. When there is reason to believe, in the opinion of Company management, that an employee is under the influence or has possession of intoxicants, nonprescription drugs or narcotics while on Company property or during working hours or that an employee has reported to work with a measurable quantity of intoxicants, non-prescription drugs or narcotics in blood or urine.
2. Work Related Accident. CyberFortress may require a drug and/or alcohol test for all employees involved in a work-related accident which results in personal injury, lost time, or property damage.
3. When Required by a Company Customer. Employees may be subject to drug testing if a Company customer requires this as a condition to work at the customer's site.

Adverse Actions

The group health insurance offered to employees and their dependents may provide limited coverage for expenses related to treatment programs. Refer to the plan description for details or contact the health insurance carrier directly. No employee will be disciplined merely for seeking assistance under such a plan. However, violations of this policy will not be excused merely because an employee is receiving treatment.

Any employee who violates any part of CyberFortress' Drug and Alcohol Abuse Policy may be subject to disciplinary action up to and including discharge.

Any employee convicted on a charge of illegal possession, use, distribution, purchase or sale of any controlled substance or alcohol, while off Company property and off duty, may be subject to discipline up to and including discharge if CyberFortress concludes that such conduct adversely affects services. In addition, CyberFortress may impose discipline up to and including discharge for such off-duty conduct in the absence of a conviction if CyberFortress has reasonable evidence of the commission of those acts and CyberFortress concludes that such conduct adversely affects services.

Any employee who is charged with a violation of any criminal drug statute must notify Human Resources within five (5) days of such charge. Criminal drug statutes include federal, state, and local laws involving the use of drugs (including controlled substances). Failure to report a charge will result in disciplinary action including termination from employment. A charge of violating any criminal drug statute may result in disciplinary action including termination.

Any employee's refusal to submit immediately upon request to a search of his/her person and/or property, or to a blood test, urinalysis, "breath-analyzer" test or other diagnostic test, may result in disciplinary action up to and including immediate discharge. A positive result on such test(s) indicating prior use of intoxicants, alcohol, non-prescribed narcotics, hallucinogenic drugs, marijuana, or other non-prescribed controlled substances may result in disciplinary action up to and including immediate discharge.

Smoke-Free Workplace

CyberFortress maintains a smoke-free and tobacco-free workplace. This includes but is not limited to cigarettes, pipes, cigars, snuff, e-cigarettes, vaping or chewing tobacco. Smoking or other use of tobacco products is NOT permitted in any part of the building or in vehicles owned, leased, or rented by CyberFortress. Employees may smoke outside **in designated areas** during breaks. No additional breaks beyond those allowed may be taken for the purpose of using tobacco or similar products. When smoking or otherwise using tobacco or similar products outside, do not leave cigarette butts or other traces of litter or tobacco use on the ground or anywhere else. Dispose of any litter properly in the receptacles provided for that purpose. While CyberFortress may provide designated areas available to smokers, it in no way has any legal responsibility to do so. Employees who choose to use these smoking areas do so at their own risk.

Workplace Violence

As the safety and security of our employees, vendors, contractors, and the public is in the best interests of CyberFortress, we are committed to working with our employees to provide a work environment free from violence, intimidation, and other disruptive behavior.

Weapons on Company property

We do not allow weapons to be carried on our premises or at CyberFortress sponsored events.

Zero Tolerance Policy

CyberFortress has a zero-tolerance policy regarding workplace violence and will not tolerate acts or threats of violence, harassment, intimidation, and other disruptive behavior, either physical or verbal, which occurs in the workplace or other areas. This applies to management, co-workers, employees, and non-employees such as contractors, customers, and visitors.

Workplace violence can include oral or written statements, gestures, or expressions that communicate a direct or indirect threat of physical harm, damage to property, or any intentional behavior that may cause a person to feel threatened.

Reporting Incidents of Violence

Report to your manager, Human Resources, or any other member of management, any behavior that compromises our ability to maintain a safe work environment. All reports will be investigated immediately and kept confidential, except where there is a legitimate need to know. You are expected to cooperate in any investigation of workplace violence.

Violations

Violating this policy may subject you to criminal charges as well as discipline up to and including immediate termination of employment.

Retaliation

Victims and witnesses of workplace violence will not be retaliated against in any manner. In addition, you will not be subject to discipline for, based on a reasonable belief, reporting a threat or for cooperating in an investigation.

If you initiate, participate, are involved in retaliation, or obstruct an investigation into conduct prohibited by this policy, you will be subject to discipline up to and including termination.

If you believe you have been wrongfully retaliated against, immediately report the matter to Human Resources.

Workers' Compensation

Workers' compensation is a no-fault system designed to provide benefits to all employees for work-related injuries. Workers' compensation insurance coverage is paid for by employers and governed by state law. The workers' compensation system may provide for coverage of medical treatment and expenses, occupational disability leave, and rehabilitation services, as well as payment for lost wages due to work related injuries. If you are injured on the job while working at CyberFortress, no matter how slight, you are to report the incident immediately to your Manager/Supervisor. Consistent with applicable state law, failure to report an injury within a reasonable period could jeopardize your claim for benefits.

To receive workers' compensation benefits, notify your Manager/Supervisor immediately of your claim. If your injury is the result of an on-the-job accident, you must fill out an accident report. You will be required to submit a medical release before you can return to work.

Please note that CyberFortress may not be liable for the payment of workers' compensation benefits for any injury that arises from your voluntary participation in any off-duty, recreational, social, or athletic activity that is not part of your work-related duties.

Incident Reporting

If an employee has an accident, injury or near-miss while on the job, they are required to report it to their manager or another member of management immediately, no matter how insignificant it may seem. Medical treatment will be promptly arranged as appropriate. If the injury is an emergency, call 911 and then your manager.

If you are involved in, or are a witness to an incident, immediate action is required – all details of the incident should be provided for reporting purposes. Failure to report or cooperate may result in a loss of benefits that might be allowed for that injury. Also, not reporting an incident may result in disciplinary action toward the party witnessing the incident and/or the direct manager. CyberFortress may require a physician's fitness for duty statement releasing the employee to return to work after any job-related injury.

Return to Work

CyberFortress is committed to promoting employee health and recovery from a work-related injury or illness through early intervention and active case management. It is our goal to maintain a safe workplace for all employees. When an injury does occur, the program helps to make the process of returning to work as smooth and efficient as possible.

This policy aims to provide meaningful work activity for all employees who become temporarily unable to perform all or portions of their regular work assignments due to work related injury or illness. To facilitate this process, return to work duties may be in the form of either changed duties within the scope of the current position, or other available duties – through CyberFortress or offsite organizations experienced in return-to-work programs.

Section 10: Personnel Records

Personal Data Changes

It is your obligation to provide CyberFortress with your current contact information, including current mailing address and telephone number. Inform CyberFortress of any changes to your marital or tax withholding status. Failure to do so may result in loss of benefits or delayed receipt of W-2 and other mailings. To make changes to this information, contact Human Resources.

Personnel Records

CyberFortress maintains a personnel file for all employees. Important events in each employee's history with CyberFortress will be recorded and kept in the employee's personnel file. Change of status records, commendations, warnings, performance improvement plans, and educational attainment records are examples of records maintained.

Every effort will be made to keep your personnel records confidential. Access is on a "need-to-know" basis only. This includes, but is not limited to, managers and others in management reviewing the file for possible promotion, transfer, or layoff. For more information on how to gain access to your personnel or medical file, contact Human Resources.

Section 11: Separation of Employment

Resignation of Employment

CyberFortress recognizes that personal situations may arise which require a voluntary termination of employment. Should this occur, CyberFortress requests that the employee provides two (2) weeks' advance notice in writing. This request does not alter an employee's at-will relationship with CyberFortress.

All rights and privileges of employment with CyberFortress terminate upon the date of separation. Terminating employees are required to return all Company property assigned to them, and provide their manager with any keys, passwords, or other means of access control to enable this Company to access its property, including computer files used while employed.

Involuntary Separation

Employees who are laid off or terminated involuntarily will be paid within the required time frame according to federal or state law. Exempt employees will be paid only for the days they worked, and not for the entire workweek.

Final Paycheck

The final paycheck will be issued within the required time frame according to federal or state law. Arrangements should be made with your payroll specialist as to whether the check will be mailed or direct deposited, and to ensure all company property has been returned and work handed off appropriately.

Exit Interview

CyberFortress will request an exit interview upon notice of termination for all Voluntary Resignations. The purpose of the exit interview is to complete necessary forms, collect Company property and discuss employment experiences with CyberFortress.

Continuation of Benefits (COBRA)

When an employee is separated for any reason, health insurance remains in effect until the last day of the month in which the separation occurred. Please contact the benefits department to inquire about any applicable COBRA or state law continuation options.

Post-Employment Verification

CyberFortress policy is to confirm dates of employment and job title only. With your written authorization, CyberFortress will confirm compensation. Forward any requests for employment verification to Human Resources.

State Addendum

The following States have additional policies that are covered in the State Addendum.

California, Florida, Indiana, Kentucky, Massachusetts, New York, Ohio, Pennsylvania, Tennessee, and Virginia.

Acknowledgment of Receipt and Review

I hereby acknowledge that I have received and read the CyberFortress Employee Handbook and the State Addendum[1] for the state in which I work. I understand that the Handbook and Addendum set forth the terms and conditions of my employment with CyberFortress as well as the duties, responsibilities, and obligations of employment with CyberFortress. I agree to abide by and be bound by the rules, policies and standards set forth in the Handbook, as well as any State Addendum that has been given or made available to me.

Employee must sign the Employee Handbook Acknowledgement for continued employment.

Employee Signature

Date