[Insert Company Name Or Logo]	
Title: Employee Responsibility for Data Security	**P&P #:**
Approval Date:	**Review: Annual**
Effective Date:	**Security Team**

Purpose: To ensure that all employees and other workforce members (whether paid, volunteer or contractor) understand their responsibilities in maintaining security of all data they have access to, or may encounter, in whatever type of format.

Scope: This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) working in all facilities under the organization's ownership.

Procedure:

The first line of defense in data security is the individual user (employee, contractor, vendor, intern). Users of Company's information systems are responsible for the security of all data which may come to them in whatever format. The Company is responsible for maintaining ongoing policy and training programs to inform all users of these requirements.

Challenge Unrecognized Personnel - It is the responsibility of all Company personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Company location, you should challenge them as to their right to be there. All visitors to Company facilities must sign in at the front office. In addition, all visitors, must wear a visitor/contractor badge. All other personnel must be employees of the facility. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Most computers will contain sensitive data either of an engineering, manufacturing, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof but do provide an additional level of security; you may request a cable lock from IT if you plan to travel out of secured locations. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all the equipment, he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. The Company requires that all computers will have the automatic

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Company Owned Assets - Only computer hardware and software owned by and installed by the Company is permitted to be connected to or installed on Company equipment or networks. This includes removable media, personal digital assistants, and smart phones/tables. Only software that has been approved for company use by the Information Technology Department (IT) may be installed on Company equipment. Personal computers (e.g., laptops, desktops) supplied by the Company are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Company for home use unless those changes are made by the Company's IT department.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Company are the property of the Company unless otherwise addressed by a contractual agreement.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred because of user action, a repetition of the action by that user may be viewed as a deliberate act.

- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or network sniffer programs and attempting to circumvent file or other resource permissions.

- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
Exception: Authorized information system support personnel, or others authorized by the Company leadership, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against malicious attacks, and system infection.

- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Company has access to customer information which is required to be protected. Certain classes of sensitive and regulated data stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

which you have not been granted access by the appropriate approval procedure is strictly prohibited.

- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on the Company's computers must be approved and installed by the IT department.

- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Company is strictly prohibited.

- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Company is strictly prohibited.

- Media Use. Using digital media owned or used by the Company to perform Company business shall not to be used on non-Company computing resources. Only media authorized by Company's IT department is authorized to be used on Company computing resources or operational technology asses.

Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, The Company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Company owned equipment are considered the property of the Company – not the property of individual users. Consequently, this policy applies to all Company employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax. As well as information saved on Company's workstations computers, laptops, and servers – to include Company provided cloud storage facilities.

Company provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible if:

1. it does not consume more than a trivial amount of employee time or resources,
1. it does not interfere with staff productivity,
1. it does not preempt any business activity,
1. it does not violate any of the following:
   a. Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
   a. Illegal activities – Use of Company's information resources for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

a. Commercial use – Use of Company's information resources for personal or commercial profit is strictly prohibited.

a. Political Activities – All political activities are strictly prohibited on Company premises. Company encourages all its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.

a. Harassment – The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, Company prohibits the use of computers, e-mail, voice mail, instant messaging, texting, and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

a. Junk E-mail - All communications using Company's IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the chain message to anyone.

While it is **NOT** the policy of the Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the company's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems, and detecting patterns of abuse or illegal activity.

The Company reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Company policies.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.

Internet Access

Internet access is provided for Company employees and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Company on Company owned computers should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use Company computers as a radio or to constantly monitor the weather or stock market results. While trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Employees are permitted to stream workplace appropriate audio/radio/media from personally owned devices via the Company's guest wireless network if it does not present a personnel safety issue.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the Company's firewall. This list is constantly monitored and updated, as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

Reporting Software Malfunctions

Users should inform the IT department when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, Company's computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or the IT department as soon as possible.

Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The IT department will monitor the resolution of the malfunction or incident, and report to senior leadership the result of the action with recommendations on action steps to avert future similar occurrences.

Report Security Incidents

It is the responsibility of each Company employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or IT professional. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, direct security of that resource. Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to the IT department.

Reports of security incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated.

Security breaches shall be promptly investigated. If criminal action is suspected, The Company's leadership may decide to contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Company and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of company policy and will result in personnel action and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on Company computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Company purchased software on home or on non-Company computers or equipment.

Company's proprietary data, including but not limited to personnel information, IT Systems information, financial information, engineering and manufacturing data or human resource data, shall not be placed on any computer that is not the property of the Company without written consent of the respective supervisor or department head. It is crucial to Company to protect all data and, to do that effectively we must control the systems in which it is contained. If a supervisor or department head receives a request to transfer Company data to a non-Company computer system, the supervisor or department head should notify the IT

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

department or appropriate personnel of the intentions and the need for such a transfer of data.

Company's Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since Company does not control non-Company personal computers, Company cannot be sure of the methods that may or may not be in place to protect Company sensitive information, hence the need for this restriction.

Internet Considerations

Special precautions are required to block Internet (public) access to Company information resources not intended for public access, and to protect confidential Company information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the IT department or appropriate personnel authorized by the Company shall be obtained before:

- An Internet, or other external network connection, is established.
- Company information (including notices, memoranda, documentation, and software) is made available on any Internet-accessible computer (e.g., website or ftp server) or device that is not owned or managed by the Company's IT department.
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor.
- Use shall be consistent with the goals of the Company. The network can be used to market services related to the Company, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including controlled unclassified information, credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g., passwords, pass phrases), shall be escrowed with IT department or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Violations: Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment, depending on the severity of the infraction. In addition, [Insert Company Name] may report the matter to civil and/or criminal authorities as may be required by law.

Attachments: None

Related Policies:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.