Port of Newport

IT Security Policy

Adopted by Resolution 2019-18
November 19, 2019

PORT OF NEWPORT
IT SECURITY POLICY

Table of Contents

Chapter 1. Passwords

1.1 Overview

(a) Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the Port of Newport's (Port) resources. All users, including contractors and vendors with access to port systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1.2 Purpose

(a) The purpose of this section is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

1.3 Scope

(a) The scope of this section includes all personnel, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any the Port's facility, has access to the Port network, or stores any public or non-public Port information. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

1.4 Password Creation

(a) All user-level and system-level passwords must conform to the Password Construction guidelines included in this Policy.

(b) Users must not use the same password for Port accounts as for other non-Port access (for example, personal ISP account, option trading, benefits, and so on).

(c) Where possible, users must not use the same password for various Port access needs.

(d) User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user to access system-level privileges.

(e) Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

1.5 Password Change

(a) All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

(b) Statement of Password Guidelines:

Strong passwords are long, the more characters you have the stronger the password. The Port recommends a minimum of 10 characters, preferably 14 in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics, and shall not be used at the Port:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

Are some version of "Welcome123" "Password123" "Changeme123"

(c) Every work account should have a different, unique password. To enable users to maintain multiple passwords, the Port will investigate 'password manager' software and once authorized will provide this to users in the Port. Whenever possible, the Port encourages the use of multi-factor authentication.

Chapter 2. Software Installation

2.1 Overview

(a) Allowing personnel to install software on company computing devices may open the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when personnel install software on company equipment.

2.2 Purpose

(a) The purpose of this section is to outline the requirements around installation software on the Port of Newport (Port) computing devices. This is intended to minimize the risk of loss of program functionality, the exposure of sensitive information contained

within the Port's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

2.3 Scope

(a) This section applies to all Port personnel, contractors, vendors and agents with a Port-owned mobile devices. This section covers all computers, servers, smartphones, tablets and other computing devices operating within the Port.

2.4 Policy

(a) Personnel may not install software on the Port's computing devices operated within the Port network, without proper authorization from the Port General manager or delegate.

(b) Software requests must first be approved by the requester's Director and then be made to the Port General Manager in writing or via email.

(c) Software must be selected from an approved software list, maintained by the Port General Manager's delegate, unless no selection on the list meets the requester's need.

(d) The delegate will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

(e) Personnel may not use a web based software for Port business that is not preauthorized by the Port. With or without authorization, all information input into the database during business hours is considered Port property and subject to the State retention schedule.

Chapter 3. Email

3.1 Overview

(a) Electronic email is pervasively used in almost all industries and is often the primary communication and awareness method within an organization. At the same time, misuse of email can pose many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications.

3.2 Purpose

(a) The purpose of this email section is to ensure the proper use of the Port of Newport's (Port) email system and make users aware of what the Port deems as acceptable and unacceptable use of its email system. This section outlines the minimum requirements for use of email within the Port's Network.

3.3 Scope

(a) This section covers appropriate use of any email sent from a Port email address and applies to all personnel, vendors, and agents operating on behalf of the Port.

3.4 Policy

(a) All use of email must be consistent with the Port's policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

(b) A Port email account should be used primarily for business-related purposes; personal communication is permitted on a limited basis, but non-Port related commercial uses are prohibited.

(c) All Port data contained within an email message or an attachment must be secured according to the Data Protection Standard.

(d) Email shall be retained according to State of Oregon Record Retention Schedule.

(e) The Port email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Personnel who receive any emails with this content from any Port personnel should report the matter to their supervisor (or Port General Manager) immediately.

(f) Users are prohibited from automatically forwarding Port email to a third party email system (noted in 4.7 below). Individual messages which are forwarded by the user must not contain Port confidential or above information.

(g) Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Port business, to create or memorialize any binding transactions, or to store or retain email on behalf of the Port. Such communications and transactions should be conducted through proper channels using port- approved documentation.

(h) Using a reasonable amount of Port resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Port email account is prohibited.

(i) Port personnel shall have no expectation of privacy in anything they store, send or receive on the company's email system.

(j) The Port may monitor messages without prior notice. The Port is not obliged to monitor email messages.

Chapter 4. Acceptable Use

4.1 Overview

(a) The Port of Newport's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Port of Newport's established culture of

openness, trust and integrity. The Port of Newport is committed to protecting its personnel, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

(b) 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 the Port of Newport. These systems are to be used for business purposes in serving the interests of the Port of Newport, and of our clients and customers in the course of normal operations.

(c) Effective security is a team effort involving the participation and support of every Port of Newport personnel 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.

4.2 Purpose

(a) The purpose of this section is to outline the acceptable use of computer equipment at the Port of Newport. These rules are in place to protect the personnel and the Port of Newport. Inappropriate use exposes the Port of Newport to risks including virus attacks, compromise of network systems and services, and legal issues.

4.3 Scope

(a) This section applies to the use of information, electronic and computing devices, and network resources to conduct the Port of Newport business or interact with internal networks and business systems, whether owned or leased by the Port of Newport, Port personnel, or a third party. All personnel, contractors, consultants, temporary, and other workers at the Port of Newport and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Port of Newport's policies and standards, and local laws and regulation. Exceptions to this section are documented in section 5.2.

(b) This section applies to personnel, contractors, consultants, temporaries, and other workers at the Port of Newport, including all personnel affiliated with third parties. This section applies to all equipment that is owned, rented or leased by the Port of Newport.

4.4 General Use and Ownership

(a) The Port of Newport proprietary information stored on electronic and computing devices whether owned or leased by the Port of Newport, Port personnel or a third party, remains the sole property of the Port of Newport. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

(b) You have a responsibility to promptly report the theft, loss or unauthorized disclosure of the Port of Newport proprietary information.

(c) You may access, use or share the Port of Newport proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

(d) Personnel 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, personnel should be guided by departmental policies on personal use, and if there is any uncertainty, personnel should consult their supervisor or manager.

(e) For security and network maintenance purposes, authorized individuals within the Port of Newport may monitor equipment, systems and network traffic at any time.

(f) The Port of Newport reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.5 Security and Proprietary Information

(a) All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

(b) System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

(c) All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

(d) Postings by personnel from a Port of Newport email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not those of the Port of Newport, unless posting is in the course of business duties.

(e) Personnel must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. Personnel shall report suspicious email to their Supervisor or Manager.

4.6 Unacceptable Use

(a) The following activities are, in general, prohibited. Personnel 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).

(b) Under no circumstances are Port of Newport personnel authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Port of Newport-owned resources.

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

(d) The following activities are strictly prohibited:

(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 the Port of Newport.

(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 the Port of Newport or the end user does not have an active license.

(3) Accessing data, a server or an account for any purpose other than conducting the Port of Newport business, even if you have authorized access.

(4) 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.

(5) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(6) 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.

(7) Using a Port of Newport 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.

(8) Making fraudulent offers of products, items, or services originating from any Port of Newport account.

(9) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

(10) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the personnel is not an intended recipient or logging into a server or account that the personnel 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.

(11) Port scanning or security scanning is expressly prohibited, unless prior authorization has been received by the Port General Manager.

(12) Executing any form of network monitoring which will intercept data not intended for the personnel's host, unless this activity is a part of the personnel's normal job/duty.

(13) Circumventing user authentication or security of any host, network or account.

(14) Introducing honeypots, honeynets, or similar technology on the Port of Newport network.

(15) Interfering with or denying service to any user other than the personnel's host (for example, denial of service attack).

(16) 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.

(17) Providing information about, or lists of, the Port of Newport personnel to parties outside the Port of Newport, except as required by law.

8.12 Email and Communication Activities

(a) When using company resources to access and use the Internet, personnel must realize they represent the company. Whenever personnel state an affiliation to the Port, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Port".

(b) The following activities are strictly prohibited:

(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 the Port of Newport's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Port of Newport or connected via the Port of Newport's network.

(7) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.8 Blogging and Social Media

(a) Blogging by personnel, using the Port of Newport's property and systems is prohibited.

(b) The Port of Newport's Confidential Information policy also applies to blogging. As such, personnel are prohibited from revealing any Port of Newport confidential or proprietary information, trade secrets or any other material covered by Port of Newport's Confidential Information policy when engaged in blogging.

(c) Personnel shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the Port of Newport and/or any of its personnel. Personnel are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Port of Newport's Non-Discrimination and Anti-Harassment policy.

(d) Personnel may also not attribute personal statements, opinions or beliefs to the Port of Newport when engaged in blogging. If personnel is expressing his or her beliefs and/or opinions in blogs, the personnel may not, expressly or implicitly, represent themselves as personnel or representative of the Port of Newport. Personnel assume any and all risk associated with blogging.

(e) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the Port of Newport's trademarks, logos and any other the Port of Newport intellectual property may not be used in connection with any blogging activity.

Chapter 5. Data Breach Response

5.1 Purpose

(a) The purpose of the section is to establish the goals and the vision for the breach response process. This section will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

(b) The Port of Newport's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how the Port of Newport's established culture of openness, trust and integrity should respond to such activity. The Port of Newport is committed to protecting the Port's personnel, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

5.2 Background

(a) This section mandates that any individual who suspects that a theft, breach or exposure of the Port of Newport protected data or sensitive data has occurred must immediately provide a description of what occurred via e-mail to dirfin@PortofNewport.com, or by calling 541-265-7758. The designated party will be responsible for contacting the information system support team to investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the appropriate procedure will be followed.

5.3 Scope

(a) This applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information (PII) or protected information (PI) of the Port of Newport personnel.

5.4 Confirmed theft, data breach or exposure of Port of Newport protected data or Port of Newport sensitive data

(a) As soon as a theft, data breach or exposure containing Port of Newport protected data or Port of Newport sensitive data is identified, the process of removing all access to that resource will begin.

(b) The Port General Manager will chair an incident response team to handle the breach or exposure.

(c) The team will include members from:

- IT Support Team (team that maintains servers)
- The Internet Service Provider (provides Firewall for the Port)
- The President of the Port Commission (or delegate)
- Director of Operations
- Director of Finance
- Legal (if applicable)
- Communications (if applicable)
- Additional individuals as deemed necessary the Port General Manager

9.10 Confirmed theft, breach or exposure of Port of Newport data

(a) The Port General Manager (GM) or delegate will be notified of the theft, breach or exposure. The Port's Internet Service Provider and/or Internet Service Provider along with the designated contractor (Forensic Investigators), will analyze the breach or exposure to determine the root cause.

(b) The Port GM or delegate will work with Forensic Investigators.

(c) As provided by Port of Newport cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or

organizations impacted; and analyze the breach or exposure to determine the root cause.

(d) The Port GM or delegate will develop a communication plan.

(e) The Port GM or delegate will work with Port of Newport communications, legal, and Board of Commissioners to decide how to communicate the breach to: a) personnel, b) the public, and c) those directly affected.

9.11 Ownership and Responsibilities

(a) Roles & Responsibilities

(1) Sponsors - Sponsors are those members of the Port of Newport personnel or contractor that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any member of the Port General Manager in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

(2) Information Security Administrator is that individual of the Port of Newport community, designated by the port General Manager, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

(3) Users include virtually all members of the Port of Newport personnel to the extent they have authorized access to information resources, and may include personnel, trustees, contractors, consultants, interns, temporary personnel and volunteers.

9.12 Enforcement

(a) Any Port of Newport personnel found in violation of this section may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

9.13 Definitions

(a) **Denial of Service Attack** - A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

(b) **Encryption or Encrypted Data –** The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

(c) **Forged Routing** - Sending packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which can degrade the functionality of the router and the network.

(d) **Honeynet** - A network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information

used to increase network security. A Honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems.

(e) **Honeypot** – A network-attached system set up as a decoy to lure cyberattackers and to detect, deflect or study hacking attempts in order to gain unauthorized access to information systems.

(f) **Hacker** – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

(g) **Information Resource** - The data and information assets of an organization, department or unit.

(h) **Network Sniffing -** A network sniffer (also known as a network analyzer, protocol analyzer or packet analyzer) is a software or hardware tool that can intercept and log traffic on a digital network. As data flows across the network, the sniffer captures each packet and, if necessary, decode the packet's raw data.

(i) **Packet Sniffing or Packet Spoofing** - The act of capturing packets of data flowing across a computer network.

(j) **Ping Flood** - A ping flood is a denial-of-service attack in which the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic.

(k) **Protected Health Information (PHI)** - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

(l) **Personally Identifiable Information (PII)** - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

(m) **Personnel** – Includes all Port of Newport full-time, part-time and temporary employees, volunteers, consultants, and Commissioners. This term is used both to mean individuals and the collective group.

(n) **Plain Text** – Unencrypted data.

(o) **Protected Data** - See PII and PHI

(p) **Safeguards** - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

(q) **Sensitive Data** - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

9.14 Policy Compliance

(a) Compliance Measurement - The Port IT contractor and identified staff will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

9.15 Exceptions

(a) Any exception to the Policy must be approved by the Port General Manager or delegate in advance.

9.16 Non-Compliance

(a) Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

References

Reserved