RESOLUTION NO. 517-09

A Resolution of the Commission of the Port of Port Townsend

RESOLUTION ADOPTING INFORMATION SECURITY POLICY

WHEREAS: the Port of Port Townsend information technology system has grown dramatically over the past decade, including a LAN currently consisting multiple servers, sixteen workstations, and at least 28 users, in five separate buildings, and;

WHEREAS: the Port has never established a comprehensive policy governing ethics, network access, computer use, security, and control of Port assets, resources and electronic information, including e-mail, internet access, passwords, and data storage, and;

WHEREAS: the Port is now working to become compliant with the new Payment Card Industry Data Security Standard (PCI DSS), to help ensure the safe handling of sensitive credit card information, with the primary purpose of attempting to reduce the risk of identity theft, and;

WHEREAS: one of the requirements of becoming compliant with PCI DSS is to have an adopted overall Information Security Policy, which will include the specific requirements of the PCI DSS, and;

WHEREAS: the Port has developed a draft of the Information Security Policy, which will become an Addendum to the Port Personal Policy Manual, and;

WHEREAS: the Port Management and Port Commission will review and update this Information Security Policy at least once a year to incorporate relevant security needs that may develop.

NOW, THEREFORE BE IT HEREBY RESOLVED the Port Commission of the Port of Port Townsend, hereby adopts the Information Security Policy, as per the attached marked "Exhibit A", Port of Port Townsend Information Security Policy.

ADOPTED this 25th day of February 2009, by the Commission of the Port of Port Townsend and duly authenticated in open session by the signatures of the Commissioners voting in favor thereof and the Seal of the Commission duly affixed.

ATTEST:

David H. Thompson, Secretary

Herbert F. Beck, President

John N. Collins, Vice President

APPROVED AS TO FORM:

Malcolm S. Harris, Port Attorney

PORT OF PORT TOWNSEND

POLICY NAME: **Administration - Information Security Policy**

EFFECTIVE DATE: **February 26, 2009** **REVISED: February 24, 2009**

1.0 INTRODUCTION

The purpose of this document is to establish the Port's policy in governing the access, use, security, and control of Port assets, resources, and electronic information. This policy covers the security of Port of Port Townsend information and must be distributed to all Port employees and selected contractors (Hereafter referred to as employee(s)).

Each employee is responsible for the security of the Port's Information Systems. Each employee must be provided with this policy and sign a form verifying that they received, read, and understand this policy.

1.1 Management's View and Enforcement of Information Security

- The Port Commission approves, adopts, and supports an information security policy and Port Management administers its enforcement. Management acknowledges that no individual is immune from investigation when there is reasonable suspicion of theft, fraud, or misuse of Port assets. Management and the Port Commission will review and update this information security policy at least once a year to incorporate relevant security needs that may develop.

1.2 Information Security Policy Objectives and Methods

- Protect against unauthorized access to a system or to the information it contains by verifying the identification of a user or entity.
- Maintain confidentiality of business information and sensitive information.
- Protect against file corruption using anti-malware software and user awareness.
- Develop a strong security posture through the creation, maintenance, and monitoring of security information such as access control policies, authorized user profiles, security parameters, and ownership identification.
- Maintain network security by preventing unauthorized access from *un-trusted* network environments through the use of firewall technology.

1.3 Ethics and Acceptable Use Policies

The Port expects that all employees conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Furthermore, an employee should report any dishonest activities or damaging conduct to their supervisor.

Port of Port Townsend computer equipment is to be used by the staff of the Port of Port Townsend for Port business and related activities including civic responsibilities and completing class assignments for Port classes and training, and authorized course work in completing requirements for fulfilling certificate requirements, or specialized course work. Computer use for performing civic responsibilities or completing class work assignments must be approved by the Executive Director, Deputy Director, or Director of Finance & Administration.

Use of computers and associated equipment is the responsibility of the assigned staff person:

- Port employees and designated contractors are allowed to use the Port's computer equipment.
- Port staff shall not use another person's logon id except in specifically defined instances. These instances are rare and require authorization by the Information Security Officer.
- Port staff not assigned to a computer workstation shall not attempt to utilize another staff person's workstation unless authorized by the assigned user.

The security of tenant, customer, and employee information is extremely important to the Port of Port Townsend. We are trusted by our tenants, customers, and employees to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information such as name, address, phone number, e-mail address, social security number, driver's license number, bank account, credit card numbers, etc. or Port information not publicly available. It is important that employees do not reveal sensitive information about our tenants, customers, and employees to outside resources that do not have a need to know such information.

The computers, e-mails, files, documents and programs are Port property. These files should not be treated or considered personal or private.

The Port of Port Townsend is a government agency, and as such, may be required to produce documentation not ordinarily disclosed by a private business. Any requests for public disclosure should be directed to the Executive Assistant.

1.4 Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees and contractors to keep security awareness levels high. The following Port policies and procedures address this issue:

- Hold information security awareness training meetings with employees and contractors to review correct handling procedures for sensitive information, as needed and at least annually.
- Employees are required to read this information security policy and verify that they understand it by signing an acknowledgement form (see Appendix A).
- Criminal history background checks will be conducted for all employees prior to employment.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Port information security policies must be reviewed annually by Port Management and Port Commission and updated as needed.

1.5 Disciplinary Action

Each employee accessing the Port's information systems is bound by the procedures detailed in this Information Security Policy. An employee's failure to comply with the standards and policies set forth in this document may result in immediate loss of computer access and disciplinary action up to and including termination of employment.

2.0 INFORMATION SECURITY

2.1 Information Security Officer

The Director of Finance and Administration is the Port's Information Security Officer.

2.2 Duties of the Information Security Officer

The Information Security Officer:

1. Provides direction and recommendations for the Information Security Policy.
2. Is responsible for communicating information security policies to employees and contractors.
3. Is responsible for monitoring and auditing all Port computer systems for compliance with the Information Security Policy and the investigation of information security compromises.
4. Provides security direction during the design and implementation phase of any application system.
5. Oversees account creation and maintenance procedures.
6. Reviews user accounts on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist.

7. Authorizes changes to the Port's firewall setup. All changes are documented and logged by the Information Security Officer.

- In the event of a compromise of sensitive information, the Information Security Officer will oversee the execution of the incident response plan.

2.3 Information Systems

Information Systems includes the Information Security Officer, and the Port computer consultant, currently Dave Olsen of Berry Hill Software, Inc.

2.4 Incident Response Plan

1. If a compromise is suspected, alert the Information Security Officer. If you are unsure whether an action details a security violation, you should report it and discuss it with the Information Security Officer.
2. Information Security Officer will conduct an initial investigation of the suspected compromise.
3. If the compromise of information is confirmed, the Information Security Officer will alert management and begin informing parties that may be affected by the compromise. If the compromise involves credit card account numbers, the Port will perform the following:

    - Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
    - Alert necessary parties such as the Port's bank, the Port's credit card processing company, the Port Attorney, the State Auditor's Office, Visa Fraud Control, law enforcement, etc.
    - Provide compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours.
    - Follow other steps listed at: http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html

3.0 ELECTRONIC MAIL (E-MAIL) POLICY

All Port employees have access to e-mail.

3.1 E-mail Purpose

The use of the Port's e-mail system provides communication between staff, external companies, tenants, customers, the public, and others. Use of the Port's e-mail is intended for business use but some personal use is allowed as described below.

3.2 E-mail Privacy

E-mail created or distributed through the Port's e-mail system is the property of the Port, and is subject to audit or monitoring. Users should be aware that under certain circumstances Information Systems staff and the Port's computer consultant may need to access and review e-mails sent and received. Additionally email is sent across the Internet in readable form. There is no guarantee of security or confidentiality when using the e-mail system.

3.3 E-mail Usage

- E-mail should be transmitted based on business need.
- The Port permits incidental personal use provided that such does not generate incremental identifiable costs to the Port and does not negatively impact the user's job performance.
- Under no circumstances is it permitted for Port employees to conduct business of any kind that would be detrimental to, or not tied directly to, the Port of Port Townsend.
- Use proper e-mail etiquette. See Attachment for a guide to email etiquette.
- Do not use e-mail to transmit messages that contain remarks, images, or content that can be considered defamatory, offensive, harassing, disruptive, derogatory, racial or ethnic slurs, or pornographic images.
- Do not use e-mail to transmit passwords or any other authentication information for the Port's systems.
- Do not use e-mail to transmit chain letters or virus hoaxes. If you are unsure about something contact Information Systems.
- Do not open e-mails with attachments that come from sources that are not recognized or when the attachment is not expected. Delete those from sources that are not recognized and confirm unusual attachments with the sender.
- Never e-mail or otherwise transmit any attachment that is suspected of being a virus.
- Inappropriate use of the e-mail system may result in immediate loss of e-mail privileges and possible disciplinary action up to and including termination of employment.

3.4 Instant Messaging

- The Port of Port Townsend does not permit the use of Instant Messaging technologies on its networks.

4.0 INTERNET USAGE POLICY

The Port of Port Townsend provides employees internet access so that they can obtain up-to-date information useful to them for the performance of their job functions and duties.

4.1 Proper Internet Usage

- All software packages and data files downloaded from non-Port sources via the internet or any other public network are automatically screened with Port-approved virus detection software.
- Information Systems must approve any modifications or additions made to any Port computer.
- No illegal or pirated information or software should be downloaded or viewed.
- Passwords transmitted or used online should be of different variations from those used within the Port.
- The Port prohibits employees from using the internet to visit sites that are pornographic, sexually explicit, racial, or ethnically biased or harassing or offensive in any way.
- The Port reserves the right to monitor any and all network activities to and from your computer including internet access. Such activities may be archived and reviewed at a future date.
- Inappropriate internet usage may result in the loss of internet access and may result in further disciplinary action, up to and including termination of employment.

5.0 SOFTWARE POLICY

Standard software applications, consistent with the needs of each employee's position, have been loaded onto his or her computer. Any modifications to this installation need to be approved by Information Systems.

5.1 Downloading and Installing Software

- All software and files downloaded from non-Port sources via the internet or any other public network is automatically screened by company approved virus detection software.
- All software downloaded or modifications made to existing software must be cleared through the Information Security Officer prior to performing any change or download.
- Only licensed software compatible with the Port's information systems will be installed on the Port's computers.
- Information Systems staff will install the software according to the Information Systems department guidelines.

6.0 NETWORK AND ACCOUNT POLICY

The Port's network consists of a multi-site computer network that includes file servers, printers, personal computers, UPS systems, fiber, V.P.N., and 100BaseT backbone cabling. File servers provide employees with access to networked applications and access to specific network locations for their directories and files.

6.1 Purpose and Account Creation

- The purpose of the Network and Account Policy is to provide a secure computer network environment for the organization's infrastructure.
  For an employee to gain Network access, the Information Systems department must receive a completed Account Request Form. The new employee's supervisor must sign the form.
- The employee's job function and department requirements will determine the level of access to network directories and applications.

6.2 Account Logins and Passwords

- Login ids and passwords control access to all Information Systems.
- The login id owner is responsible for all actions performed by their login id.
- All accounts require both a username and a password.
- User ids, accounts, or passwords may not be shared with another person under any circumstances except in specifically defined instances authorized by the ISO. You are required to report any unauthorized incident of id, account, or password sharing.
- Network passwords must be changed every 90 days.
- All passwords must be a minimum of 7 characters.
- Passwords should not be a real word that can be found in the dictionary.
- Passwords should contain a combination of letters, numbers, and characters.
- User will be locked out after three failed logins. The account will be locked for 30 minutes or until reset by a member of Information Security.

6.3 Account Modification

- The Information Systems department must receive a completed Account Change Request Form to change an employee's level of network access. The employee's supervisor must sign the form.
- The employee's job function and department requirements will determine the level of access to network directories and applications.

6.4 Account Removal

- Upon termination of employment, an employee's network and e-mail access must be disabled immediately. After 30 days the account will be deleted.

7.0 PHYSICAL SECURITY

Restrict physical access to sensitive information or systems that house that information, such as computers or filing cabinets storing cardholder data, to protect it from those who do not have a need to access that information. Media is defined as any printed or handwritten paper, received faxes, floppy disks, backup tapes, computer hard drives, etc.

- Media containing sensitive information must be securely handled and distributed.
- Media containing stored sensitive information, especially credit card account numbers and social security numbers, should be properly inventoried and disposed of when no longer needed for business by deleting, shredding, overwriting, or degaussing before disposal.
- Visitors should always be escorted and easily identifiable when in areas that may contain sensitive information.
- Each employee should log off the Marina Program and MAS 90 Accounting system when leaving their computer. Each employee should lock their computer (CTRL-ALT-DEL), when leaving it for longer than 10 minutes.
- All computers will automatically lock themselves after 15 minutes of inactivity.
- Each employee should be aware of social engineering, the manipulation of employees to gain information for the purpose of perpetrating fraud or damage to the system.

8.0 DATA USER RESPONSIBILITIES

8.1 Protect Stored Data

Protect sensitive information stored or handled by the company and its employees. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business reasons. Any media, such as paper, floppy disk, backup tape, computer hard drive, etc., that contains sensitive information must be protected against unauthorized access. Media no longer needed must be destroyed in such a manner to render sensitive data unrecoverable such as shredding, overwriting, degaussing, disassembly, etc.

8.2 Credit Cardholder Data Handling Specifics

Protecting cardholder data is an important goal of the Port of Port Townsend (Port). The Port recognizes the importance of minimizing the amount and types of cardholder data retained and limiting the number of people with access to cardholder data.

8.2.1 Purpose

The purpose of this policy is to establish a standard for protecting cardholder data.

8.2.2 Scope

The scope of this policy includes all Port personnel, contractors, consultants, etc who have access to or are responsible for accepting or processing cardholder data. Cardholder data is defined in section 6 but in brief includes credit/debit card numbers, expiration dates, and similar credit card/debit card information.

8.2.3 General

- Do not store sensitive credit card data.
- Mask the PAN when displayed.
- Do not send unencrypted PANs by end-user messaging technologies
- Access to cardholder data is limited to authorized personnel.
- Paper and electronic media containing cardholder data must be labeled and stored and transported securely.

8.2.4 Requirements

A. Do not store sensitive credit card authentication data after authorization.
   1. Do not store the full contents of any track from the magnetic stripe on the back of the card.
   2. Do not store the card-validation code
   3. Do not store the personal identification number (PIN) or the encrypted PIN block.

B. The PAN must be masked when displayed
   1. Only display the last 4 digits of the PAN

C. Do not send unencrypted PANs by end-user messaging technologies
   1. Do not use Email, Instant Messaging, Chat, FTP, or similar technologies to transmit unencrypted PANs.
   2. Do not transmit unencrypted PANs via any method that has not been authorized by a signed Port directive.

D. Access to cardholder data is limited to authorized personnel.
   1. Access to cardholder data and the system components supporting cardholder data shall be restricted to those individuals whose jobs require such access.
   2. A record of which individuals have authorized access to cardholder shall be maintained.
   3. If employees obtain customer's credit card information over the telephone, the transaction must be processed immediately, and the paper on which the information is written must be shredded immediately after processing.

E. The security of paper and electronic media containing cardholder data must be maintained:
   1. Media containing cardholder data shall be classified and labeled as 'Confidential'.
   2. Media containing cardholder data shall only be transported by a method that can be accurately tracked.

3. Media containing cardholder data shall be stored securely.

F. Management approval must be obtained prior to moving media containing cardholder data from a secure area.

G. Media containing cardholder data shall be stored in restricted access areas. These areas shall have locking doors and shall be restricted from access by the public and unauthorized personnel.

H. Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons.
   1. Hardcopy materials shall be cross-cut shredded, incinerated, or pulped so that data cannot be reconstructed.

8.3 Protect Data in Transit

If sensitive information needs to be transported physically or electronically, it must be protected while in transit between Port Offices, to a storage facility, or across the internet.

Credit Card Handling Specifics

- Due to the lack of security of e-mail, credit card account numbers must never be e-mailed.
- Media containing credit card account numbers must only be given to trusted persons for transport between Port Offices or to off-site locations.
- Logging sheets are to be used for tracking these moves.

8.4 Restrict Access to Data

Restrict access to sensitive information to those that have a need-to-know. No employees should have access to credit card account numbers unless they have a specific job function that requires such access.

9.0 VIRUS DETECTION SOFTWARE

- All desktop computers and network servers have Port-approved virus detection software.
- All desktop computers are configured to have the virus detection scan periodically for viruses.
- All desktop computers are configured to have the virus detection software download and update the virus definitions on a periodic basis.

- Users must not cancel automatic virus scanning or updating of definitions. If such automatic activity interferes with the user's duties, the user should contact the Information Security Officer for additional support.
- All software and files downloaded from non-Port sources via the internet or any other public network is automatically screened by company approved virus detection software.
- Users should never e-mail or otherwise transmit any attachment that is suspected of being a virus.

10.0 SOCIAL ENGINEERING

- Social engineering is the manipulation of employees to gain information for the purpose of gaining access to commit fraud or damage to the system.
- Shoulder surfing is watching over the shoulder of a user while they login or execute a sensitive program. Users should use caution when executing sensitive programs or entering login information.
- Janitorial recovery is retrieving documents discarded in the wastebasket or recycle bin, or copying documents left in unlocked drawers. Users should use caution with sensitive documents and be sure to shred sensitive documents when discarding.
- Password grabbing is using a program or procedure that looks like a normal logon process but instead records the user's password and user name. Users should log off workstations when away to avoid such activity.

11.0 WIRELESS NETWORKS

- All wireless networks and wireless network devices must be approved by Information Systems before installation.
- Inappropriate use of wireless networks may result in disciplinary action, up to and including termination of employment.

12.0 DEFINITIONS

Terms	Definitions
Cardholder data	1) Full magnetic stripe or the PAN plus any of the following: * Cardholder name * Expiration date * Service Code (http://selfservice.talisma.com/display/2n/_index1.aspx?tab=glossary&r=0.1504929) 2) all personally identifiable data about the cardholder and relationship to the Member (i.e., account number, expiration date, data provided by the Member, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other personal insights gathered about the cardholder (i.e., addresses, telephone numbers, and so on)." (http://www.sfs.finance.ucla.edu/survey/glossary.htm)
Primary Account Number (PAN)	Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number. (http://selfservice.talisma.com/display/2n/_index1.aspx?tab=glossary&r=0.1504929)
PIN Block	Encrypted Personal Identification Number

13.0 REVISION HISTORY

February 25, 2009 - Resolution No.517-09 approved by Port Commission.

PORT OF PORT TOWNSEND
AGREEMENT TO COMPLY WITH INFORMATION SECURITY POLICIES

Employee Name _____

I agree to take all reasonable precautions to assure that Port of Port Townsend sensitive data or information, that has been entrusted to the Port of Port Townsend by third parties such as tenants and customers, will not be disclosed to unauthorized persons. At the termination of my employment with the Port of Port Townsend, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Executive Director or Deputy Director.

I have access to a copy of the Information Security Policies. I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by these policies and other requirements found in the Port's Information Security Policy. I understand that non-compliance may be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I agree to promptly report all violations or suspected violations of the Information Security Policy to the designated Information Security Officer.

Employee Signature _____

Date _____

Port of Port Townsend
Account Request/Change Form

User Information:

Name (Last, First, MI)	
Date of Hire	
Department/Location	
Supervisor's Name	

Access Requirements:

Network		E-mail	
Internet		Voice Mail	
Marina Program		Other	
MAS 90			

Approval:

Supervisor's Signature	
Date	

Prior to setting up a new information systems account, employees must read and understand the Port's Information Security Policy, and agree to comply with the Policy. Please attach a signed copy of the Agreement with the request.

Access Completed:

Completed By	
Date Completed	

Port of Port Townsend email etiquette guidelines

- Be concise and to the point
- Answer all questions, and pre-empt further questions
- Use proper spelling, grammar and punctuation
- Make it personal
- Use templates for frequently used responses
- Answer swiftly
- Do not attach unnecessary files
- Use proper structure and layout
- Do not overuse the high priority option
- Do not write in CAPITALS
- Don't leave out the message thread
- Add disclaimers to your emails
- Read the e-mail before you send it
- Do not overuse Reply to All
- Take care with abbreviations and emoticons
- Be careful with formatting
- Take care with rich text and HTML messages
- Do not forward chain letters
- Do not request delivery and read receipts
- Do not ask to recall a message
- Do not copy a message or attachment without permission
- Do not use emails to discuss confidential information
- Use a meaningful subject
- Use active instead of passive
- Avoid using URGENT and IMPORTANT
- Avoid long sentences
- Don't send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks
- Don't forward virus hoaxes and chain letters
- Keep your language gender neutral
- Don't reply to spam