

Table of Contents

Information Technology Security Policy

1. Purpose	1
A. Security Concerns	1
B. Shared and Trusted Environment.....	2
2. Scope	3
A. Security Definition	3
B. Team Effort.....	3
C. Applicability/Enforcement	3
3. Security Policies and Responsibilities	4
A. Elected Office/Departments.....	4
B. Information Technology Committee	5
C. Internal Auditor	5
D. Central Services (Information Services Division)	5
E. System Administrators.....	6
F. Security Policies for System Users.....	6
Resolution No. 12612	8

1. Purpose

A. Security Concerns

The purpose of this Information Technology (IT) Security Policy is to establish standards to maintain system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse, damage to, or loss of data. The county's dependence on local area networks (LANs), wide area networks (WANs) and the Internet for conducting vital public business has highlighted the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information;
- Physical Security – Limiting access to servers, network equipment, and workstations.
- Network access points – Limiting access to Thurston County's network only through entry points approved by Central Services with security controls in place.
- Misuse - The use of information or systems for other unauthorized purposes;
- Information Browsing - Unauthorized access to sensitive information by intruders or legitimate users;
- Hacking and Penetration - Attacks by unauthorized persons or systems that may result in denial of service, damage to systems, loss of productivity, or significant increases in incident handling costs;
- Computer Viruses and Worms – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in loss or falsification of data;
- Component Failure - Failure due to design flaws or hardware/software faults which can lead to denial of service or security compromises through the malfunction of a system component; and
- Employee Education and Awareness – The need to educate Thurston County employees about computer systems in order to limit inadvertent corruption, loss and unauthorized access of electronic information.

B. Shared and Trusted Environment

- 1) Because information technology security planning is primarily a risk management issue, this policy and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:
 - System wide approaches to end-user authentication;
 - Consistent and adequate network, server, and data management recognizing the interdependent relationship of county offices;
 - Appropriate uses of secure network connections; and
 - Closing unauthorized pathways into the network and into data exempted from public disclosure.
- 2) Information Security should be viewed from a county wide approach. In order to succeed, the county offices and departments should adhere to the following principles:
 - Require adherence to common security architecture and its related procedures;
 - Recognize an interdependent relationship among departments, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
 - Assume mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.
- 3) In response to security concerns, departments must take the necessary steps to:
 - Ensure secure interactions between and among governmental agencies and county departments take place within a shared and trusted environment;
 - Ensure secure interactions between and among business partners, external parties, state agencies and county departments utilize a common authentication process for logging in to systems, security architecture, and points of entry;
 - Prevent misuse of, damage to, or loss of IT hardware and software assets;
 - Ensure accountability for protection of IT assets; and
 - Prevent unauthorized use or reproduction of data.

2. Scope

A. Security Definition

For the purposes of this policy, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by Thurston County and to protect IT assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of IT facilities and off-site data storage; computing, telecommunications, and applications related services purchased from other government agencies or commercial concerns; and Internet-related applications and connectivity.

B. Team Effort

To be effective, information security must be a team effort involving the participation and support of every individual who deals with Thurston County information and/or information systems.

C. Applicability/Enforcement

This policy applies to all county offices, departments, officials, employees and all system users.

Every system user at Thurston County -- no matter what their status (employee, contractor, consultant, temporary, etc.) -- shall comply with the information security policies found in this policy and the standards and guidelines developed by the Information Technology Committee (ITC). Employees who deliberately violate this and other information technology policy statements will be subject to disciplinary action up to and including termination.

This policy applies to all computer and network systems owned by and/or administered by Thurston County. Similarly, this policy applies to all platforms (operating systems), all computer sizes (personal computers through mainframes), and all application systems (whether developed in-house or purchased from third parties). The policy covers only information handled via computers and/or networks.

Thurston County reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of Thurston County information systems, which adversely affects the ability of others to use these information systems, or which is harmful, offensive, or inappropriate will not be permitted.

3. Security Policies and Responsibilities

A. Elected Office/Departments

All Elected Offices and Departments will:

- 1) Implement compliance checking to ensure that organizational units are operating in a manner consistent with the Information Technology (IT) Security Policy, Standards and Guidelines, and developed security procedures of Thurston County.
- 2) Request, as soon as possible, any system user that leaves Thurston County to be removed from all known systems. This includes but is not limited to permanent employees, temporary and project employees, interns, volunteers, and contractors.
- 3) Periodically check system user lists to assure accuracy for current employee access.
- 4) Request access from Central Services for employees only for systems needed for specific job tasks. Request from Central Services to have employee's access removed from systems that are no longer needed for job tasks.
- 5) Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard against security breaches.
- 6) Train staff to follow security procedures and standards.
- 7) Train staff on the use of software and hardware to prevent or reduce accidental data loss or corruption.
- 8) Ensure appropriate security measures are included when purchasing or developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce).
- 9) Ensure and oversee compliance with adopted security standards and procedures
- 10) Implement recommended security guidelines as adopted by the Information Technology Committee (ITC) when possible.
- 11) Ensure all supervisors, working in conjunction with Human Resources, take appropriate disciplinary or other measures to address violations of information security requirements.

B. Information Technology Committee

The Information Technology Committee will:

- 1) Establish organization-wide information security standards, guidelines, and procedures.
- 2) Review all IT security policies, standards and guidelines at least annually and make appropriate updates after significant change in business, computing or computing environment.
- 3) Communicate security policies, standards and guidelines to county offices and departments through the established communities of interest sub-committees.

C. Internal Auditor

The Internal Auditor will:

- 1) Conduct IT Security Policy and Standards Compliance Audit periodically.
- 2) Review developed security standards and guidelines.
- 3) Assist in developing security procedures for newly implemented technology.

D. Central Services (Information Services Division)

Central Services Information Services staff will:

- 1) Propose security standards and guidelines for adoption by the ITC including new standards and guidelines for emerging technologies and business changes.
- 2) Write detailed security procedures for supporting adopted security standards.
- 3) Ensure and oversee compliance with adopted security standards and procedures for Information Technology personnel. This task will require testing network or system security, including use of industry cracking tools or methods.
- 4) Offer training for staff in adopted security standards.
- 5) Investigate system intrusions and other information security incidents in coordination with the Prosecuting Attorney's office and / or Internal Auditor.

E. System Administrators

All system administrators (including Central Services staff and department/office staff that have specific duties as system administrators) will:

- 1) Follow the current information technology security standards and guidelines.
- 2) Implement information technology security standards and guidelines within the parameters of each system they are responsible for. If a situation arises that is not included in the current security standards and guidelines, a request to Central Services should be made to augment or modify the standards and guidelines.
- 3) Inform system users of security requirements for each specific system.
- 4) Provide any training necessary or answer questions to make sure end users understand the security standards and guidelines and make recommendations to elected officials and department directors to improve security.

F. Security Policies for System Users

All system users will be assigned a unique user login name (User-ID) and password to access the county's network. Multiple User-IDs and passwords may be required to access additional systems related to specific job tasks. This policy applies to permanent, temporary, project, volunteer, contract or intern staff that needs access to systems. Users of any system at Thurston County will:

- 1) Maintain security of assigned login names and passwords for various systems. If access to a system is no longer needed, system users need to request from their supervisor to be removed.
- 2) Be held responsible for any activity transacted under the individual's User-ID. Take precautions to protect passwords from unauthorized individuals.
- 3) Ensure against unauthorized access when leaving a workstation unattended by logging off systems or using screen saver passwords.
- 4) Follow security standards and guidelines for maintaining and changing passwords.
- 5) Report any security compromise or suspected security compromise to supervisor AND Central Services immediately.

- 6) Be prohibited from using unapproved or unauthorized hardware or software designed to compromise or crack (hack) security, passwords or encrypted data.
- 7) Contact the system administrator or Central Services if security training is needed.
- 8) Keep assigned computers and files free from viruses; make sure diskettes, especially from outside sources, are virus free.
- 9) Not take steps to circumvent or avoid system security.
- 10) Be familiar with county information technology policies and standards. These are located on the Intranet at:
<http://intra.co.thurston.wa.us/itc/policy>
- 11) Sign a statement agreeing to comply with this policy.

RESOLUTION NO. 12612

A Resolution adopting an Information Technology Security Policy to be included in the Thurston County Administrative Manual.

WHEREAS, the Thurston County Board of Commissioners wishes to establish standards to maintain system security, data integrity and confidentiality of information held by the County; and

WHEREAS, the Board wishes to protect information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction; and

WHEREAS, the Board believes the best way to accomplish these goals is to adopt an Information Technology Security Policy;

NOW, THEREFORE, THE BOARD OF COUNTY COMMISSIONERS OF THURSTON COUNTY, WASHINGTON HEREBY RESOLVES AS FOLLOWS:

Section 1. The Information Technology Security Policy attached hereto and incorporated herein by reference is hereby adopted for inclusion in the Thurston County Administrative Manual.

Section 2. If any provision of this Resolution or its application to any person or circumstance is held to be invalid, the remainder of this resolution and its application to other persons or circumstances shall not be affected.

ADOPTED: October 16, 2001

ATTEST:

Laborita J. Bouymal
Clerk of the Board

APPROVED AS TO FORM:

EDWARD G. HOLM
PROSECUTING ATTORNEY

By: Jane Futterman
Jane Futterman
Deputy Prosecuting Attorney

BOARD OF COUNTY COMMISSIONERS
Thurston County, Washington

[Signature]
Chairman

[Signature]
Commissioner

Excused absence
Commissioner