

**AUTHORIZING A SKAGIT COUNTY INFORMATION TECHNOLOGY SECURITY
POLICY**

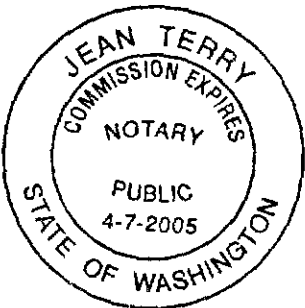
WHEREAS, the Skagit County Board of County Commissioners wishes to establish standards to maintain system security, data integrity, and confidentiality of information held by the County; and

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 BE IT RESOLVED AND IT IS HEREBY ORDERED by the Board of Skagit County Commissioners, State of Washington, that the Information Technology Security Policy attached hereto and incorporated herein by reference is hereby established.

IN TESTIMONY WHEREOF WE HEREUNTO SET OUR HAND AND AFFIX THE OFFICIAL SEAL OF OUR OFFICE this 15th day of April 2002.



**SKAGIT COUNTY, WASHINGTON
BOARD OF COUNTY COMMISSIONERS**

Don Munks
Don Munks, Chairman

Kenneth A. Dahlstedt
Kenneth A. Dahlstedt, Commissioner

Ted W. Anderson
Ted W. Anderson, Commissioner

ATTEST:

Joanne Giesbrecht
Joanne Giesbrecht, Clerk of the Board

Joanne Giesbrecht

Skagit County

Information Technology Security Policy



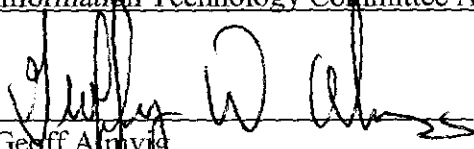
Created: February 21st, 2002

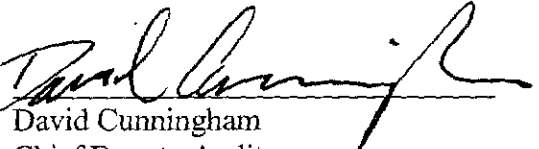
Skagit County


Information Technology Security Policy


Approvals

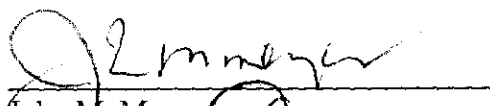
Information Technology Committee Approvals:



Geoff Almvig
Geographic Information Services Manager


David Cunningham
Chief Deputy Auditor



Mark Leander
Assessor



Tom Verge
Prosecutor

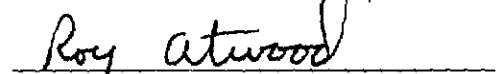

John M. Meyer
Superior Court Judge


Cori Russell
Records Manager

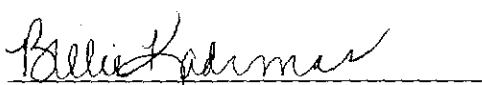

Tim Holloran
Senior Services Director



Michael Almvig, (non-voting)
Information Services Director


Rick Smith, Director (non-voting)
Skagit Emergency Communications Center


Roy Atwood (non-voting)
Administrative Officer

Approved as to Form Only:


Billie Kadmas, Risk Manager


Stacy Thomas
Civil Litigator Deputy

Information Technology Security Policy

Adopted by the Skagit County Board of County Commissioners (SCBCC), March, 2002.

Effective: Immediately

Table of Contents

1	Definitions.....	1
2	Purpose.....	2
2.1	Security Concerns.....	2
2.2	Shared and Trusted Environment.....	3
2.3	Enterprise Wide Approach.....	3
3	Scope.....	3
3.1	Security Definition.....	4
3.2	Team Effort.....	4
3.3	Involved Persons.....	4
3.4	Involved Systems.....	4
3.5	Primary Departments Working on Information Security.....	4
4	Security Policies and Responsibilities.....	5
4.1	Elected Office/Departments/Associate Partners.....	5
4.2	Information Technology Advisory Committee.....	5
4.3	Information Services.....	6
4.4	System Administrators.....	6
4.5	System Users.....	6
5	Specific Information Technology Security Policies.....	7
6	Maintenance.....	7

1 Definitions

Peripheral Device – Any device that is connected either directly or indirectly to the Skagit County network. Examples of such devices include, but are not limited to; scanning devices, digital cameras, printing devices, Personal Digital Assistants, and modems.

Skagit County Network – The collection of computers, peripheral equipment, telecommunication equipment, and cable infrastructure that is owned and/or operated by Skagit County.

Associate Partner(s) – Any agency, political subdivision, private company or contractor that has been given access to the Skagit County Network.

Worker – Any individual who utilizes Skagit County computers or resources to conduct business on behalf of Skagit County or its Associate Partners. A worker may not necessarily have access to Skagit County's private network.

User – An individual who has been granted an account on Skagit County's private network. An example of a user may be a Skagit County or Associate Partner employee, contractor, volunteer, or any other person who has been authorized to access Skagit County's private network.

2 Purpose

2.1 Security Concerns

The purpose of this Information Technology (IT) Security Policy is to create an environment within Skagit County that maintains system security, data integrity and privacy by preventing unauthorized or illegal access to data and by preventing misuse of, damage to, or loss of data. The county's transition from proprietary network connections over dedicated leased networks to 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 Skagit County's network through defined entry points with security controls in place.
- Misuse - The use of information assets for other than authorized purposes by either internal or external users;
- Information Browsing - Unauthorized access to sensitive information by intruders or legitimate users;
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service 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 financial loss or embarrassment to the organization.
- Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component.
- Employee Education and Awareness – The need to educate Skagit County employees on security awareness and use of computer systems in order to limit the inadvertent corruption, loss, unauthorized access of electronic information.

2.2 Shared and Trusted Environment

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:

- Common approaches to end-user authentication;
- Consistent and adequate network, server, and data management;
- Appropriate uses of secure network connections; and
- Closing unauthorized pathways into the network and into data exempted from public disclosure.

2.3 Enterprise Wide Approach

Such an environment is made possible through an enterprise approach to security in County government that:

- Promotes an enterprise view among separate departments and Associate Partners;
- Requires adherence to a common security architecture and its related procedures;
- Recognizes an interdependent relationship among departments, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
- Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.

In response to these threats and to assist county departments and Associate Partners in mitigating associated risks, the SCBCC requires that departments and Associate Partners take steps necessary to initiate an enterprise-wide approach 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, security architecture, and point of entry;
- Prevent misuse of, damage to, or loss of IT hardware and software facilities;
- Ensure employee accountability for protection of IT assets; and
- Prevent unauthorized use or reproduction of copyrighted material.

3 Scope

3.1 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 Skagit 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.

This policy applies to all county departments that operate, manage or use IT services or equipment to support critical county business functions.

3.2 Team Effort

To be effective, information security must be a team effort involving the participation and support of every worker who deals with information and/or information systems. In recognition of the need for teamwork, security policy standards and guidelines will clarify the responsibilities of users as well as the steps that Skagit County must take to help protect information and information systems.

3.3 Involved Persons

Every worker at Skagit County -- no matter what their status (employee, contractor, consultant, temporary, outside agency, etc.) -- must comply with the information security policies found in this document and any other Skagit County Security documents. Employees of Skagit County who deliberately violate Skagit County Board of Commissioner adopted Information Technology policies may be subject to disciplinary action up to and including termination per Skagit County's PERSONNEL POLICIES AND PROCEDURES Manual. Associate Partner employees or other users who deliberately violate this and other information technology policies may have their rights of access to the Skagit County Network revoked.

3.4 Involved Systems

This policy applies to all computers, peripheral devices and network systems owned by and/or administered by Skagit 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.

3.5 Primary Departments Working on Information Security

Guidance, direction, and authority for information security activity for all Skagit County organizational units is the responsibility of the SCBCC. The SCBCC has created the Information Technology Advisory Committee (ITAC), which will advise the board on

establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of the elected officials and department directors. Investigations of system intrusions and other information security incidents is the responsibility of the Information Services Department in coordination with the Prosecuting Attorney's office. Department Head/Elected Official or Associate Partner managers are responsible for disciplinary matters resulting from violations of information security requirements.

4 Security Policies and Responsibilities

4.1 Elected Offices/Departments/Associate Partners

All Elected Offices, Departments, and Associate Partner(s) will:

1. Operate in a manner consistent with the Skagit County Security Policy, Standards and Guidelines, and developed security procedures of Skagit County.
2. Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and computer data computing and telecommunications facilities -- including telephones, hardware, software, and personnel -- against security breaches.
3. Train staff to follow security procedures and standards.
4. Train staff on the use of software and hardware to prevent or reduce accidental data loss or corruption.
5. Ensure appropriate security measures are included when purchasing or developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce).
6. Ensure and oversee compliance with adopted security standards and procedures
7. Adopt and implement recommended security guidelines when possible.
8. Comment on recommended changes to the IT security policy or standards and guidelines within 30 business days of a draft release from the Information Technology Committee.
9. Conduct Departmental or Agency IT Security Policy and Standards Compliance Audit annually per the Skagit County Information Technology Security Standards and Guidelines.
10. Review developed security standards and guidelines.
11. Assist in developing security procedures for newly implemented technology.

4.2 Information Technology Advisory Committee

The Information Technology Advisory Committee will:

1. Review all IT security policies, standards and guidelines at least annually and make appropriate updates after significant change(s) in the business, computing or telecommunications environment(s).
2. Communicate security policies, standards and guidelines to county offices and departments through the established communities of interest.
3. Review comments from department heads and elected officials regarding draft changes to the IT security policy or standards and guidelines, incorporate such comments into the current draft or facilitate conflicts between drafts and received comments.
4. Prepare final versions of security policies, standards and guidelines for submission to the Skagit County Board of Commissioners for approval by resolution.
5. Conduct, in conjunction with Information Services under oversight of the Board of County Commissioners, security audits to determine if policies, standards, and guidelines are being adhered to. The ITAC, may commission an outside audit agency to perform this function.

4.3 Information Services

Information Services staff will:

1. Write information technology security policies, standards and guidelines for adoption by the ITAC and SCBCC.
2. Write detailed security procedures for supporting adopted security standards.
3. Ensure and oversee compliance with adopted security policies, standards and procedures for Information Technology personnel.
4. Research and recommend new policies, standards and guidelines for emerging technologies or business changes.
5. Work with County departments and Associate Partners to train staff in adopted security policies, standards and guidelines.

4.4 System Administrators

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

1. Make every effort possible to seek, learn, and understand the current information technology security policies, standards and guidelines.
2. Ensure the policies, standards and guidelines are followed within the parameters of each system they are responsible for. If a situation arises that is not included in the current security policies, standards and guidelines, a request to Information Services should be made to augment or modify the standards and guidelines.
3. Inform users of security requirements for each specific system.
4. Provide any training necessary or answer questions to make sure users understand the security standards and guidelines.

4.5 Users

Any users or workers that utilize county owned information technology equipment and data will:

1. Adhere to and follow to the best of their abilities communicated security policies, standards and guidelines.
2. Seek assistance from the system administrator if training is needed or questions arise concerning security.
3. Skagit County Employees may not take steps to circumvent or avoid system security (Per the county Personal Policy Manual Section 22). Associate Partner employees may not take steps to circumvent or avoid system security (per contract stipulations between Skagit County and Associate Partner).

5 Specific Information Technology Security Policies

Specific security standards and guidelines will be found in the *Information Technology Security Standards and Guidelines*. This document will be the responsibility of the ITAC to maintain and may be modified as business or security needs arise. At a minimum the Information Technology Security Standards and Guidelines will be reviewed on an annual basis.

6 Maintenance

Technological advances and changes in the business requirements of county offices and departments will necessitate periodic revisions to policies, standards, and guidelines. Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will be recommended by ITAC and require the approval of the Skagit County Board of County Commissioners.