

Policy Type: Information Technology
Policy Title: Information Technology Security
Policy Number: IT-01

Purpose:

The purpose of the IT Security policy is to ensure compliance with DIS policies. It covers the security of IT facilities, data, off-site data storage, computing and telecommunications equipment, application-related services purchased from other state agencies or commercial concerns, and Internet-related applications and connectivity.

Scope:

This policy applies to Green River employees, facilities and services.

Definitions:

For the purposes of the Green River Information Technology Security Policy, security is defined as the ability to protect:

1. The integrity, availability, and confidentiality of information assets managed by Green River,
2. Information assets from unauthorized release or modification, and accidental or intentional damage or destruction, and
3. Technology assets (infrastructure) from unauthorized use.

Policy or Procedure:

It is the IT Security Policy of Green River that:

1. Green River shall operate in a manner consistent with the goals of the DIS IT Security Policies to maintain a shared, trusted environment for the protection of sensitive data and business transactions. Green River shall provide secure business applications, infrastructures, and procedures for addressing the business needs of the college.
2. Furthermore, Green River will provide services with the following principles in mind to promote the shared security of the system:
 - a Green River shall assure that appropriate security standards are considered and met when developing or purchasing application systems or data access tools;
 - b Green River shall recognize and support the necessity of authenticating external parties prior to granting access to sensitive information and applications;
 - c Green River shall develop and follow security standards for securing workstations, servers, telecommunications, and data access within its network; and
 - d Green River shall follow security standards established for creating secure sessions for application access.
3. Each application developed or purchased by Green River after August 2003, must include an architectural document offering an overview of its high-level structure and design, as well as

details of the security considerations in design, implementation, and use of the application. This will be reviewed by the Green River Security Administrator and a selected group of developers as early in the process as possible, but no later than implementation. Due to the high-risk nature of these applications, this requirement will apply to all (new and existing) Internet-based applications supported by Green River. This document will be incorporated into the portfolio of Green River Security Policy documentation and used for security validation and audit purposes.

4. Green River will ensure all staff are trained in IT security awareness, and that technical staff receive the appropriate training commensurate with their job responsibilities.
5. Green River will review its IT security processes, procedures, and practices annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment.
6. Green River will conduct a compliance audit of its IT Security Policy and Standards consistent with state requirements. Knowledgeable parties independent of Green River IT staff, such as the State Auditor, must perform the audit. The work shall follow audit standards developed and published by the Auditor. The State Auditor's office may determine an earlier audit of some or all of Green River IT processing is warranted, in which case they will proceed under their existing authority. The nature and scope of the audit must be commensurate with the extent that Green River is dependent on secure IT to accomplish its critical business functions. Green River will maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit. To the extent that the audit documentation includes valuable formulae, designs, drawings, computer source codes, object codes or research data, or that disclosure of the audit documentation would be contrary to the public interest and would irreparably damage vital government functions, such audit documentation is exempt from public disclosure. See RCW 42.17.310 and 42.17.330.
7. Pursuant to RCW 43.105.017(3), the Vice President of Information Technology is responsible for the oversight of Green River IT security and will confirm in writing that the agency is in compliance with this policy. The annual security verification letter will be submitted to the ISB, as required. The verification indicates review and acceptance of Green River security processes, procedures, and practices as well as updates.
8. The State Auditor may audit Green River IT security processes, procedures, and practices, pursuant to RCW 43.88.160 for compliance with this and DIS IT policy.

Green River IT security standards and practices contain information that may be confidential or private regarding Green River business, communications, and computing operations or employees. Persons responsible for distribution of these documents should consider the sensitive nature of the information as well as the related statutory exceptions from public disclosure See RCW 42.17.310 and 42.17.330.

Specific Authority: This policy exercises the exemption granted in the DIS IT Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200.

Law Implemented:

History of Policy or Procedure

Draft: October 15, 2004

Adopted: April 5, 2005

Revised:

Reviewed by:

Contact: Carolyn Hershberger, Vice President, Information Technology, ext. 3317

President's Staff Sponsor: Carolyn Hershberger, Vice President, Information Technology, ext. 3317