Green River College

Information Technology
Security Program Plan

This page left blank intentionally

Green River College (GRC)
Information Technology Security Program Plan

Table of Contents

SCOPE - Higher Education Exemption

The Green River College Information Technology Security Program applies to all employees, students, and other authorized users of college information technology resources.

Institutions of higher education shall develop standards that are appropriate to their respective missions and that are consistent with the intended outcomes of the Washington State CIO and WaTech (Washington Technology Solutions) to secure data, systems and infrastructure. At a minimum, higher education institutions' security standards shall address:

a. Appropriate levels of security and integrity for data exchange and business transactions.
b. Effective authentication processes, security architectures(s), and trust fabric(s).
c. Staff training.
d. Compliance, testing, and audit provisions.

Furthermore, the GRC IT Security Program Plan is guided by the Northwest Commission on Colleges and Universities (NWCCU) Accreditation Standards, with a special focus on Standard 2.I.1

> "Consistent with its mission, the institution creates and maintains physical facilities and technology infrastructure that are accessible, safe, secure, and sufficient in quantity and quality to ensure healthful learning and working environments that support and sustain the institution's mission, academic programs, and services."

The objective of the Green River College Information Technology Security Program is to safeguard the maintenance, confidentiality, integrity and availability of GRC information and systems. This is done through appropriate levels of security for data exchange; authentications for access; and appropriate staff training.

The Green River College Information Technology Security Program must be reviewed at least annually, and any identified areas of improvement must be documented as part of the review.

As an institution of higher education, Green River College (GRC) operates independently from the Washington State Digital Government framework. GRC is not part of the State Government Network (SGN).

1. GRC IT Security Program

1.1 Documentation

1.a Oversight Accountability

The Information Security Officer under the direction of the Executive Director of Information Technology has the responsibility of overseeing the college's information technology resources and operations including:

- Establishing procedures, guidelines and policies for the security practices of IT personnel.

- Establishing procedures, guidelines and policies for the security practices for users of computer services.
- Establishing procedures, guidelines and policies for the physical security of IT equipment.
- Establishing information technology security awareness and training programs.
- Reviewing and approving information technology purchases to ensure they meet institutional standards for support and security.
- Reviewing capital projects for physical IT security that is appropriate to the college.
- Establishing standards for common authentication processes, security architecture and point of entry.
- Auditing the security program to ensure that the security program contains comprehensive practices that emphasize the importance of preventing unauthorized access, misuses, modification, damage to or loss of IT hardware, software, data and facilities.
- Reviewing assessments conducted for IT project submittals to compare the risk level with the authentication mechanism. IT project submittals will be initiated using the IT Project Request Form and the IT Project Charter form.

1.b Information Technology Oversight Support

Information Technology, led by its Executive Director, is subdivided into the following teams which support the GRC IT Security Program Plan in the indicated manner:

Administrative Services	Managers are responsible for oversight of their teams, including training, processes, and compliance. Staff are responsible for hardware/software inventories, shipping/receiving, purchasing, and project management.
Dev Ops Application & Data Integration Services	Responsible for business and administrative systems development, implementation, support, version control, testing and project management practices. Maintains expertise in software development and project management.
Enterprise Services	Responsible for desktop configuration, virus technologies, server administration and operations, common authentication strategies, and encryption strategies. Maintains expertise in enterprise software, hardware, storage, operating systems, application security, encryption techniques, and other security strategies.
Information Security	Responsible for creating, managing, and implementing IT security policies, processes, and procedures, as well as preventing, investigating, and recovering from security incidents and data breaches.
IT Employee Service Desk	Responsible for initial tech support, customer service, and case creation for employee technology issues.

Network / Telecom Services	Responsible for network administration and operations, switches, routers, wireless access, physical wiring, communications technologies, and firewall configuration. Maintains expertise in network infrastructures and firewalls.
Security	Responsible for establishing security related standards, procedures, guidelines, and policies. Responsible for reviewing capital projects for physical IT security. Responsible for auditing the security program and reviewing the assessments conducted for IT project submittals.
Service Operations and Incident Management Group	Responsible for computer, laptop, printer, media equipment, and peripheral support and repair. Receives new and disposes of old computing equipment. Maintains expertise in desktop computing and troubleshooting. Only works on GRC owned equipment. Does not support personally owned devices or network connections.
Student Technology Support Desk	Responsible for supporting student technology issues while on a GRC campus. Provides assistance with GRC student account access and network connection. Does not troubleshoot personally owned devices beyond assistance with connecting to a GRC wireless network. Does not work on GRC employee equipment.

The college manages the installation of software on operational servers and workstations via a change control process. Software upgrades are proposed via a change request. The timing and method of changes are reviewed and approved by the ASC (Administrative Systems Committee) and INTEC (Instructional Technology) Committees.

Job descriptions for these teams include:

- Executive Director of IT
    - Executive Assistant
    - Information Security Officer
        - IT Security
    - Integration, Data Governance & Solutions Manager
        - Software Engineer
        - Web Architect
    - IT Customer Support Director
        - Customer Service Manager
            - Student IT Customer Support
        - IT Customer Support
    - IT Project Manager
    - IT Technical Services Director

- IT Network and Telecommunications
- IT System Administration

1.c Mechanism of Enforcement

The Executive Director of Information Technology is the hiring authority and director for IT personnel with responsibility for the tasks described above.

The primary mechanism of enforcement regarding the security practices and IT purchases of users in other departments is the purchasing approval authority of the Executive Director of Information Technology. This authority covers both IT purchases and service contracts.

1.d Information Asset Overview

This section is designed to provide an overview of Green River College's information assets. Green River College's information assets fall into the following categories:

Employment Data	Much of the salary and employment data housed in payroll and human resource systems is a matter of public record. However, social security numbers, benefits information, home addresses and phone numbers do qualify as protected information. These data require a high degree of protection from disclosure.
Enrollment Data	Enrollment Services maintains pre-admissions student directory information, student directory information, enrollment data and student transcript data. These data require a high degree of protection from disclosure and modification.
Financial Aid Data	The office of Financial Aid maintains information in support of application for and disbursement of student grants, loans and scholarships. This includes educational, demographic and tax information including social security numbers, student and parent income, aid eligibility, awards and disbursements. These data require high degree of protection from disclosure and modification.
Financial Data	Purchasing, accounts receivables, general ledger and bank statements. These data require a high degree of protection from modification and financial account information requires a high degree of protection from disclosure.

Health Data	GRC operates a Counseling Services department run by faculty and a Nursing Program to train students. The Counseling Services department retains notes of their counseling sessions, and this data requires a high degree of protection from data disclosure and modification. Currently, the Nursing Program does not maintain medical records. If at any time the Nursing Program begins to collect medical records, this data will require a high degree of protection from data disclosure and modification.
Police Services Data	Incident and case files typically associated with law enforcement. These data require a high degree of protection from data disclosure and modification.

1.e Governing Regulations

FERPA	The Family Education Rights and Privacy Act protects the privacy associated with student educational records. Data includes student demographics, enrollment, financial aid, and grievance data.
GDPR	The European Union's General Data Privacy Regulation (GDPR) governs protection of data of EU citizens. It mandates the right of the user to proactively grant approval to collect data, the right to be informed of collected data, and the right to be forgotten.
Gramm-Leach-Bliley Act	Governs protection of information for consumers of financial services. This includes Financial Aid loans and collections. Mandates the establishment and on-going maintenance of an IT Security Plan to protect consumer information.
Higher Education Act	The Higher Education Act governs most aspects of the disbursement of financial aid. Checks be issued within ten days of receiving awards. Prolonged disruption of financial aid systems carries potential legal and fiscal liabilities.
HIPAA	The Health Insurance Portability and Accountability Act (HIPAA) defines the Federal Privacy requirements for health care data.
PCI-DSS	Payment Card Industry Data Security Standard (PCI-DSS) governs protection of credit card information.
RCW 70.02	Washington State interpretation and application of HIPAA governing health care data.

The Patriot Act	Governs release of data under specific cases where a subpoena or search warrant is issued for student information, requiring us to maintain confidentiality of such requests.

1.f Equipment Approval Process

The Executive Director of Information Technology retains signature authority on all IT purchases, including workstations, servers, network equipment, software, telecommunications devices and all other technology solutions. The Information Security Officer reviews all new IT purchases to verify compatibility, security, and accessibility. The following guidelines are used to approve equipment purchases:

- Network and telecommunications equipment is reviewed for compatibility and security by the Network/Telecom Services team.
- Servers, enterprise software, and storage equipment is reviewed for compatibility and security by the Enterprise Services team.
- Workstation, laptop, and tablet models, and desktop peripherals are approved for compatibility and security by the Desktop Support team.

1.2 IT Risk Assessment

1.2.a Risk of Disclosure

Green River College uses the following risk categories in defining the risk of disclosure:

Low	Information in this category should not contain data that can be related to the identity of an individual, result in a negative fiscal impact to the institution, or adversely impact operations. Information typical of this category is accounting information, statistical information, procedures, policies, published regulations, directories, advertising, etc.
Medium	Unauthorized disclosure of information may have a negative operational impact or is classified as “personally identifiable”, but does not carry legal or fiscal liability, and cannot lead to identity theft.
High	Unauthorized disclosure of information would constitute a violation of federal or state law, constitute an invasion of privacy, result in harm to the individual or carry significant financial liability. Examples of information in this category include student enrollment data, health related information, and police case and evidentiary files.

1.2.b Risk of Modification

Green River College uses the following risk categories in defining and identifying the risk of modification of data:

Low	The college does not anticipate any significant negative operational, fiscal or legal impacts associated with unauthorized data modification.
Medium	Unauthorized modification of data could constitute significant negative operational and/or fiscal impact to the college, such as the modification of financial records.
High	Unauthorized modification of information would constitute a violation of federal or state law, result in harm to the individual or carry serious financial liability. Examples of information in this category include financial accounting data, health related information, and police case and evidentiary files.

1.2.c Risk of Disruption

Green River College uses the following category definitions to identify operational criticality and the corresponding risk associated with sustained disruption of service:

Low	Denial of service for the system or application could be accommodated for a significant period of time (1 week or more) without serious operational impact, fiscal or legal liability.
Medium	Denial of service for periods of time up to a week would have significant financial or operational impact or affect the delivery of curriculum.
High	Denial of service for short periods (<72 hours) would have significant negative financial, legal or operational impacts.

1.2.d System/Application Risk Overview

The following table indicates the IT systems that are used to manage the various information assets, along with the highest level of risk associated with the data contained in the application for each of the risk categories (Disclosure, Modification and Disruption).

System	Disclosure	Modification	Disruption	Assets Contained
Canvas	High	Medium	Low	Student Enrollment, Student Transcript
ctcLink	High	High	High	Student Enrollment, Financial Aid, HR/payroll
EAB Navigate	High	High	Medium	Financial History, Non-public records,

				Educational Materials, In-process evaluations
Network File Storage	High	High	High	Financial History, Non-public records, Educational Materials, In-process evaluations
SQL	High	High	High	Student Enrollment, Financial History, Non-public records, Educational Materials, In-process evaluations
Online Collaboration & Storage	High	High	High	Employee & Student data, files, chat, and other communications in OneDrive, SharePoint, etc.

1.2.e Health and Counseling Data

Green River College operates a student Counseling Center and has a student nursing program but does not maintain any personally identifiable health records.

1.2.f Threat Assessment

The following summarizes the spectrum of known or common threats to infrastructure, data and services based on historical assessment and environmental factors.

Earthquake	Green River College is located in a geologically active area of the state. Significant seismic events occur every few years. Hardware failure and water damages are likely to occur during earthquakes.
Fire	Green River College has many trees and other vegetation around campus that could be fuel for a fire. The fire suppression system in the GRC datacenter is a water sprinkler and will cause serious harm to the equipment, high potential for data loss, and possible electrocution to anyone in the room if it is deployed.
DOS (Denial of Service) Attacks	Green River College is regularly targeted for DOS attacks. Processes and equipment have been implemented to minimize the impact of these kinds of attacks.
Fraud	Green River College has recorded no instances of IT fraud. However, the institution recognizes the need to maintain protections against the fiscal liability associated with this threat.

Human Error	Data and program backup practices minimize the impact of data loss associated with this threat.
Phishing	Green River College is regularly targeted with phishing scams and many users fall victim to this and provide their account credentials. This is a severe risk to the college and its data.
Terrorism	Green River College acknowledges a small risk associated with activities that might be classified as terrorism. There is historical precedence of bomb threats, active shooters on campus, etc.
Theft	Green River College's role as a public institution makes theft control a challenging problem because there is a desire to make IT resources available off hours and easily accessible to the general student population.
Viruses / Worms / Malware	Anti-Virus/Malware controls have minimized the disruption and damage caused by these outbreaks.
Volcano	Primary concern about volcano damage comes from the proximity of our campuses to Mt. Rainier. In the event of a major eruption, ash and lahar could damage our campuses.
Water Damage	Primary concern about water damage comes from accidental discharge of fire suppression system, water line or HVAC leaks associated with equipment failure or earthquake damage.

1.2.1 Design Review

GRC will perform a security design review for maintenance and new development of systems and infrastructure projects when one or more of the following conditions exist:

(1) A GRC project or initiative impacts risk to state IT assets outside the college.

(2) A GRC project or initiative meets criteria for a Design Review as defined and documented by the GRC IT Security Program Plan.

1.3 IT Security Assessment

GRC conducts periodic IT Security Assessments to review and assess the effectiveness of existing security controls. These assessments must include testing of security controls to make sure unauthorized access attempts can be identified or stopped. Examples of periodic testing include penetration tests, vulnerability assessments and system code analysis.

1.3.a Significant Infrastructure Upgrades

See **Appendix 1.3.a** for a list of significant IT infrastructure upgrades or modifications since the last IT Security Assessment was performed. This list will be updated upon completion of any stage of internal or external review processes.

1.4 Education and Awareness

Green River College will:

(1) Ensure that personnel assigned responsibilities defined in the GRC IT Security Program Plan are competent to perform the required tasks.

(2) Document the knowledge, skills, and abilities required for personnel performing work affecting the GRC IT Security Program Plan.

(3) Require that all employees receive annual security awareness training that includes the risks of data compromise, their role in prevention, and how to respond in the event of an incident as relevant to the individual's job function.

(4) Ensure that personnel assigned responsibilities defined in the GRC IT Security Program Plan must, at a minimum, receive training that addresses the WaTech IT Security and Privacy Awareness Training Policy, the college's security policies and procedures, and any training required by regulations that apply to their job duties.

1.5. Compliance

Green River College will:

(1) Select and apply the appropriate security controls commensurate with the risk and complexity of the system after completing the college IT Risk Assessment (Section 1.2), IT Security Assessment (Section 1.3), and the GRC IT Software Security Checklist to comply with the requirements in the WaTech IT security standards.

(2) Require contractor's compliance with WaTech IT security standards relative to the services provided when:

   a. The scope of work affects a college IT resource or asset.

   b. The college contracts for IT resources or services with an entity not subject to the WaTech IT security standards.

      Contractor compliance may be demonstrated by mapping comparable contractor controls to these IT security standards, and by adding supplemental controls that close gaps between the two.

(3) Confirm in writing that the college is in compliance with WaTech IT security standards. The head of each college will provide annual verification to WaTech by August 31 of each year or Office of Financial Management budget submittal date, whichever is later, that a GRC IT Security Program Plan has been developed and implemented according to the WaTech IT security standards. The annual security verification letter will be included in the college IT portfolio and submitted to WaTech and the Washington State CIO. The verification indicates review and acceptance of college security policies, procedures, and practices as well as updates since the prior verification.

1.6. Audit

GRC will ensure an independent audit is performed once every three years to assess compliance with WaTech IT security standards.

(1) Ensure the audit is performed by qualified parties independent of the college's IT organization.

(2) Submit the results of the audit to the state CISO (Chief Information Security Officer) at WaTech.

(3) Maintain documentation showing the results of the audit according to applicable records retention requirements.

(4) Validate that security controls are implemented appropriately based on WaTech IT security standards, the college security program, and applicable regulatory requirements.

(5) Identify nonconformities and related causes.

(6) Track progress to correct nonconformities.

(7) Implement the corrective action needed.

1.7. Maintenance

GRC will:

(1) Conduct an annual maintenance and review of the GRC IT Security Program Plan.

(2) Identify areas to improve the effectiveness of the GRC IT Security Program Plan.

1.7.a Security Program Accountability

Information Technology retains the authority for ensuring that Green River College's IT Security Program Plan is properly maintained and periodically evaluated.

1.7.b Program Update/Review

1.7.b.1 Periodic Review/Evaluations

The following procedures will be followed in support of the mandated periodic evaluation of Green River College's IT Security Program Plan:

1. Every spring the Information Security Officer will coordinate annual evaluations.
2. The Information Security Officer will review tasks and milestones identified in the previous review and/or audit for completion. These will be collected for inclusion in the annual security verification letter.
3. The Executive Director of IT will review the new standards and identify areas that require coordination with Data Guardians for additional review.
4. A list of identified tasks for continued compliance with the GRC IT Security Program Plan will be maintained (a list of current nonconformities and deviations).
5. Upon successful completion of the evaluation, the Executive Director of IT will complete the annual security verification letter, as mandated by the policy to be completed prior to August 15th of each year.

1.7.b.2 Project Initiated Evaluations

In order to facilitate the timely update of the security program, and to ensure that new security practices are documented, Green River College will identify projects that have potential security program impacts. Projects will be evaluated or identified by the Information Security Officer:

Such projects include, but are not limited to:

- Capital projects as they may alter standards around physical security.
- Implementation of new systems.
- Projects to substantially alter or redesign network or telecommunications infrastructure.
- Implementation of a new business office or function that tracks additional data domains.
- Addition of new Internet-based information systems.

Potential design or program modification tasks will be added to section 0 as they are discovered.

1.7.b.3 Procedure for Changes

The following procedure will be followed for changes to the Security Program:

1. A data guardian or information technology manager brings forward the proposed change or issue.
2. The change is reviewed by the Information Security Officer and assigned to an individual or group for follow-up.
3. A task is added to the Compliance Activities Pending-Completed document to ensure documentation in the plan.
4. Concurrent with the change in practice, the plan is updated, and the task is marked as completed on the Compliance Activities Pending-Completed document.

1.7.c IT Security Plan Maintenance History

See **Appendix1.7.c** for a list of pending and completed compliance activities. This task list will be updated upon completion of any stage of internal or external review processes.

1.7.d Program Dissemination

Upon completion of revisions to the Security Program, it will be posted where the appropriate people can access it, including the following:

- Information Technology staff
- Key information technology related staff not contained in Information Technology such as the Senior Director of College Relations and Director of Institutional Effectiveness.

2. Personnel Security

These Personnel Security controls are designed to reduce risks of human error, theft, fraud, or misuse of facilities.

2.a Acceptable Use Policy

Green River College has adopted an Acceptable Use Policy which applies to all college IT system users as well as any and all equipment connecting to the college network. This policy governs the use of any and all college owned or managed computer systems (such as, web pages, all forms of software, hardware and associated peripherals), as well as personally owned equipment that is connected to the college network. Violations of the Acceptable Use Policy may result in the loss of access to college IT resources and/or college disciplinary actions, civil proceedings and/or criminal proceedings.

2.b Secure Email

Green River College does not currently implement a "secure email" system. The appropriate use policy restricts sending of confidential information across the Internet via unencrypted email. Users have other options for sending confidential or sensitive data securely or can manually select the option to encrypt their email thread to provide greater security.

2.c Acceptable Use of Technology and Data Policy

See **Appendix 2.c** for a link to the Acceptable Use of Technology and Data policy.

2.1 Security Awareness Orientation/Training

GRC follows the WA State WaTech SEC-03 "IT Security and Privacy Awareness Training Policy" with regards to annual security awareness training.

2.1.1 Training Aims

Green River College supports a variety of security related training programs that are designed to meet the following goals:

- Educate users of computers and computer systems about the risks associated with general use of e-mail and Internet services.
- Educate those with access to protected information about the responsibilities of maintaining confidentiality of protected data as it relates governing regulations.
- Educate employees about appropriate stewardship practices as well as appropriate/ethical uses of state resources.

2.1.2 Antiviral Awareness

Green River College uses periodic e-mails to keep users abreast of current and past computer virus risks. These e-mails include tips for avoiding viruses and malware as well as notifications of specific risks or events as they occur.

2.1.3 FERPA Training

Access to systems containing data protected by the Family Education Rights and Privacy Act require training and a signature verifying that the individual is trained in the issues associated with the handling of FERPA protected information.

2.1.4 Security Awareness Training

Security Awareness Training is discussed during New Employee Orientation sessions and is immediately made available to new employees and assigned annually to current employees. Periodic emails are sent to remind staff of security protocols as needed.

2.1.5 Training Frequency

Training frequencies and schedule vary according to the training activity as follows:

FERPA Training	Once upon gaining access to systems with protected data.
Ethics Training	Required for all employees every 3 years.
Antiviral Awareness	Whenever exposure to a virus outbreak is high and no less than once per year.
Security Awareness	Annually for existing staff and assigned at New Employee Orientation for new faculty/staff. Also made optionally available quarterly to students.

2.1.6 Future Training Goals

As the complexity and interactive nature of information technology increases, GRC recognizes the need to update training materials pertaining to the following topics:

- Best practices for protecting Green River College's IT resources including hardware, software and facilities
- Password protection practices
- Accountability for software licensing programs
- Appropriate location of data and storage
- Security of email training
- Document retention

2.2 Security Program Orientation

All new Information Technology staff members will be oriented using the security program document as a guide.

See **Appendix 2.2** for information regarding the IT Security Awareness Training process.

2.3 IT Security Support Personnel, New Hires, Terminated and Vendors

For a list of GRC IT Security Support Personnel, New Employees hired during the past year, Employees terminated, or a list of Vendor Contracts during the past year; please see the Executive Director of Information Technology or the Vice President for Business Administration and Human Resources.

2.4 Hiring Practices

Information Technology follows the practices as defined in the Classified Employee Hiring Checklist provided by human resources. These include the following tasks:

- Written IT job descriptions (including minimum performance requirements and required skills),
- Application examinations to verify skills and experience
- Reference Checks prior to offering position

2.5 Reference /Background Checks

Reference checks are conducted for all Information Technology staff to include asking the former supervisors to verify employment history and the candidate's representation of their skills.

The hiring of system and network administrators, includes questions specific to the following topics:

- Employee history with following security guidelines.
- Employee history in handling sensitive information.
- Employee history in risk assessment decisions.

In all cases, questions are tailored to the individual's background as indicated on the employment applications.

Human Resources through Washington State Patrol manage background checks for all permanent staff. Where appropriate, background checks are conducted for temporary and student employees.

2.6 Employee Performance Requirements

Information Technology uses the Washington State Personnel Development Plan process for evaluating all employees. An evaluation and assessment is performed 3 months after employment begins. When used in IT positions, the process includes a definition of performance expectations and regular performance measurements surrounding the following key attributes:

- Following rules and procedures surrounding established security practices and procedures.
- Using good judgment, particularly surrounding tasks that involve risk of data.

2.7 IT Security Support Staff Technical Training

2.7.1 Training Aims

IT security support staff training programs will achieve the following goals:

- Ensure that Internet application developers are trained on writing secure applications for the web.
- Ensure that System administrators are kept abreast of current security vulnerabilities and potential solutions.

2.7.2 Informal Training Practices

We routinely seek to send IT staff to conferences that incorporate current IT security topics. Employees sent to these conferences are instructed to share key learning regarding security with other IT support staff.

2.7.3 Threat Awareness

All systems administrators are required to maintain current subscriptions on security mailing lists. Each individual is responsible for forwarding information on security trends and threats to the Information Security Officer and other system administrators on campus.

2.8 Vendor Confidentiality Agreements

Information Technology service and support contracts are processed through the GRC purchasing department and based on a DES (Department of Enterprise Services) template and always includes language regarding maintaining confidentiality of data as well as providing security awareness

2.9 Vendor Monitoring

Visitation to the campus data centers and network closets is restricted, and visitors must be accompanied at all times by Information Technology staff.

All vendor access to applications/installations is restricted. Temporary access is granted via session sharing or a limited use network logon if on campus and is supervised at all times by Information Technology or facilities staff. Access is never granted to confidential data without a signed data sharing agreement.

2.10 Contractor Contract Exhibit

See **Appendix 2.10** for a list of contractors and vendors recently used by IT.

2.11 Separation from GRC

See **Appendix 2.11** for a list of recent employee separations.

3. Physical and Environmental Protection

GRC is responsible for ensuring that adequate physical security and environmental protections are implemented to maintain the confidentiality, integrity, and availability of the GRC computer systems. GRC will take steps necessary to prevent unauthorized access, damage, or compromise of IT assets. Investments in physical and environmental security must be commensurate with the risks, threats, and vulnerabilities unique to each physical site and location.

3.1. Facilities

3.1.1 Data Center/Network Closet Security attributes

This section describes the physical security associated with the college Data Centers and Network Closets.

3.1.2 Location and Layout

All Data Centers and Network Closets (with one exception of one at a remote campus location) are located in secure environments with limited physical access. The primary data center is located on the first floor of the Library building. Layout and location have been designed with the following basic security characteristics:

- Facility is located on the first floor of the Library building, well out of traffic patterns.
- Auto-starting backup generator and a room UPS provide power protection.

3.1.3 Access Control

To enter the primary data center, one must use a proximity key card to open the door and the key card system logs each entry using the unique IDs assigned to authorized staff.

3.1.4 Communications Equipment

Physical access to network and telecommunications equipment is controlled with either traditional lock and keys mechanisms or proximity key cards. The Executive Director of Information Technology authorizes the issuance of keys. The Director of Facilities must also approve issuance of master keys.

3.1.5 Secure Location of Equipment

All server, network and telecommunications equipment is kept in locked data centers or data communication closets. The Executive Director of Information Technology or the Director of Facilities must authorize issuance of keys to these rooms/closets.

3.1.6 Protection of Physical Network Infrastructure

Network cabling is concealed above suspended ceilings or in wall. Revisions to physical cabling infrastructure must be approved by Information Technology prior to implementation.

3.1.7 Off-site media storage

Green River College utilizes a cloud based, immutable backup solution that automatically replicates all backup data to multiple cloud repositories. Data transfers are end-to-end encrypted.

3.1.8 Mobile Computing Security Controls

Laptops, notebooks, and tablet computers have been identified as "small and attractive" and have an increased risk of theft. The following security practices have been developed to guard against these risks:

- Devices are clearly marked as "The Property of Green River College".
- Each device is assigned either an Washington State Identification number or an GRC identification number, which is printed on a label on the casing.
- Inventory of this equipment is performed bi-annually.

4. Data Security

Data security components outlined in this section are designed to reduce the risk associated with the unauthorized access, disclosure, or destruction of GRC data.

Data Security Policy Statements

Green River College has developed the following codified data security related policy statements:

- WAC 132j-126 Rules of student conduct
- WAC 132j-164 Buckley Family Educational Rights and Privacy Act Policy
- WAC 132j-276 Public Records

4.1. Data Classification

GRC classifies data into categories based on the sensitivity of the data. GRC data classifications must translate to or include the following classification categories:

(1) Category 1 – Public Information

Public Information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

Public Information data includes the mission/vision/values of an agency, information related to obtaining services, staff phone numbers, work e-mail addresses, budget information, and FERPA "directory information" designated at Green River College as FERPA information at level 1.

Electronic transfer of data in this classification is not restricted.

(2) Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Sensitive data should not be transferred outside the GRC network electronically unless on password protected media or via encrypted email or encrypted file transfer. You must be specifically authorized to transfer such data outside the agency. Transfer inside the GRC network is allowed.

Specific examples include, but are not limited to:

- Data Warehouse data unless that data falls under a Category 3 or 4 classification
- Student Directory Information as per FERPA regulations can be disclosed to outside organizations with the student's prior consent or released during a public records request of Data Warehouse data.
- Certain personnel records – e.g., misconduct records subject to public disclosure
- Public Employee Financial information, but not salaries as this is public information
- Directory Information includes:
    - Student name
    - Student birthplace and birthdate
    - Student address
    - Student telephone number
    - Student e-mail address
    - Major field of study (EPC)
    - Dates of attendance (YRQ)
    - Degrees and awards received
    - Photograph
    - Participation in officially recognized activities or sports
    - Height and weight of athletes
    - Most recent educational agency or institution attended
    - Other similar information
- Directory information does NOT include:
    - Social security number
    - Student identification number
    - Race
    - Ethnicity
    - Nationality
    - Gender
    - Class schedule
    - Course and Program information not tied directly to a student, such as:

- Department and Course Number
- Course Title
- Course Intent
- Program Code (EPC)
- Program Title

(3) Category 3 – Confidential Information

Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

a. Personal information about individuals, regardless of how that information is obtained such as home address, phone number, and personal e-mail address
b. Information in employee personnel records including evaluations
c. Information regarding IT infrastructure and security of computer and telecommunications systems
d. All financial data not included in the Public Employee Financial Information data
e. Personal network user information (e.g., usernames and passwords)
f. Enrollment information protected under FERPA such as:
   1 Student Information Numbers (SIDs)
   2 Grades
   3 Courses taken
   4 Test scores
   5 Educational services received

This category of data can be transferred internally, with appropriate care – e.g., via encrypted email, via Teams, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the agency via encrypted or password protected media. You must be specifically authorized to transfer such data outside the agency and there must be a signed confidentiality agreement with that individual or company prior to sending the information.

SBCTC Definition of Category 3 Data:

Enrollment information protected under FERPA, personnel and financial data. Category 3 includes all data elements except those explicitly stated in categories 2 and 4. Category 3 data is not distributed unless governed by a contract or data sharing agreement. This information is protected due to:

a) *Sensitivity – Information which must be protected due to proprietary, ethical, contractual or privacy considerations.*
b) *Legal Obligations – Information for which disclosure to persons outside of the SBCTC may be governed by specific standards and controls designed to protect the information such as FERPA.*
c) *Moderate risk – Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the SBCTC or college reputation, violate and individual's privacy rights, or make legal action necessary.*

This information includes but is not limited to:

- *Student Identification Numbers (SID)*
- *Grades*
- *Courses taken*
- *Test Scores*
- *Educational services received*
- *Bio-demographics (e.g., race, gender, family status, employment status)*
- *All personnel data including salaries*
- *All financial data*

Confidential Information data includes personal network user information, data related to IT security, employee and student personal information such as ID number, home address, phone number, personal email address, including information designated as Green River College FERPA levels 2 & 3.

This category of data can be transferred internally, with appropriate care – e.g., marked in email as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the college via password protected or encrypted media. You must be specifically authorized to transfer such data outside the college.

Specific examples include, but are not limited to:

- *Personnel records. – e.g., Evaluations*
- *Employee personal Information – e.g., home address, home email, home phone*

Note: Student email (personal or Green River Student Email) is not considered an internal transfer.

(4) Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements (such as FERPA, HIPAA, or PCI-DSS)
b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions

Confidential Information Requiring Special Handling includes employee or student information such as social security number, date of birth, etc., and information designated as Green River College FERPA level 4.

Specific examples include, but are not limited to:

- Banking/Financial Account information
- Records protected by PCI-DSS such as Credit Card Numbers
- Employee and Student Social Security Numbers
- Date of birth
- Student Identification Numbers (SID)
- Academic records of matriculated students
- Educational records protected by FERPA
- Medical records protected by HIPAA
- Medical Records, including psychological/counseling records

This category of data can be transferred internally, with appropriate care – e.g., via encrypted email, via Teams, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the agency via encrypted or password protected media. You must be specifically authorized to transfer such data outside the agency.

4.2 Data Sharing

4.2.1 Inter-agency Cooperation

Green River College does not share data with other agencies or vendors except where required by law or where Green River College has entered into a legal contract with specific language that meets or exceeds our data security standards. Data may also be shared in response to legal public disclosure requests and where required by law.

Before sharing Category 3 and above data outside GRC, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address the following:

(1) The data that will be shared
(2) The specific authority for sharing the data
(3) The classification of the data shared
(4) Access methods for the shared data
(5) Authorized users and operations permitted
(6) Protection of the data in transport and at rest
(7) Storage and disposal of data no longer required
(8) Backup requirements for the data if applicable
(9) Other applicable data handling requirements

4.3 Secure Management and Encryption of Data

4.3.1 Storage Encryption Practices

In general (with the exception of sensitive data in databases), Green River College does not employ encryption "at rest" and chooses to employ appropriate access controls for confidential data. Any data encrypted on storage devices are encrypted using industry standard algorithms and practices that are commensurate with the nature of the data and risk factors. File storage data stored on network shares is not encrypted, but rather protected by file access control lists (ACL's). Database servers have a variety of authentication/authorization methods to protect access to sensitive data and encryption enabled for sensitive data. Users are instructed through Security Awareness Training to store all data that has a medium or greater risk of disclosure or modification on approved network file or database servers. Users are also instructed that portable data storage devices are not approved secure storage devices.

4.4 Secure Data Transfer

All GRC data must be transferred securely and via a GRC approved method. Non-GRC provided or approved transport options (e.g., an employee sending GRC data to or via their personal email account or through a personal social media account) are not permitted.

4.4.1 Transmission Encryption Practices

Encryption risk assessment processes are enforced for all applications which transit the Green River College firewall.

4.4.2 Public/Private Key encryption

GRC will utilize Public/Private key encryption for automated internet applications with the following basic attributes:

- Automated file transfers facilitated with PGP-FTP.
- Private and Public keys managed by Enterprise Services staff
- Private Keys stored in a private directory that is only accessible by Enterprise Services staff.
- An automated process responsible for encryption and decryption of data.

4.4.3 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is required for securing user interactive HTTP sessions during transmission of the following types of data:

- Web applications/sessions that prompt users for username and passwords or contain session keys that could be used to circumvent authentication/authorization
- Data that is classified with a medium or high risk of disclosure.
- Interactive web applications that are classified with a medium or high risk of modification.

5. Network Security

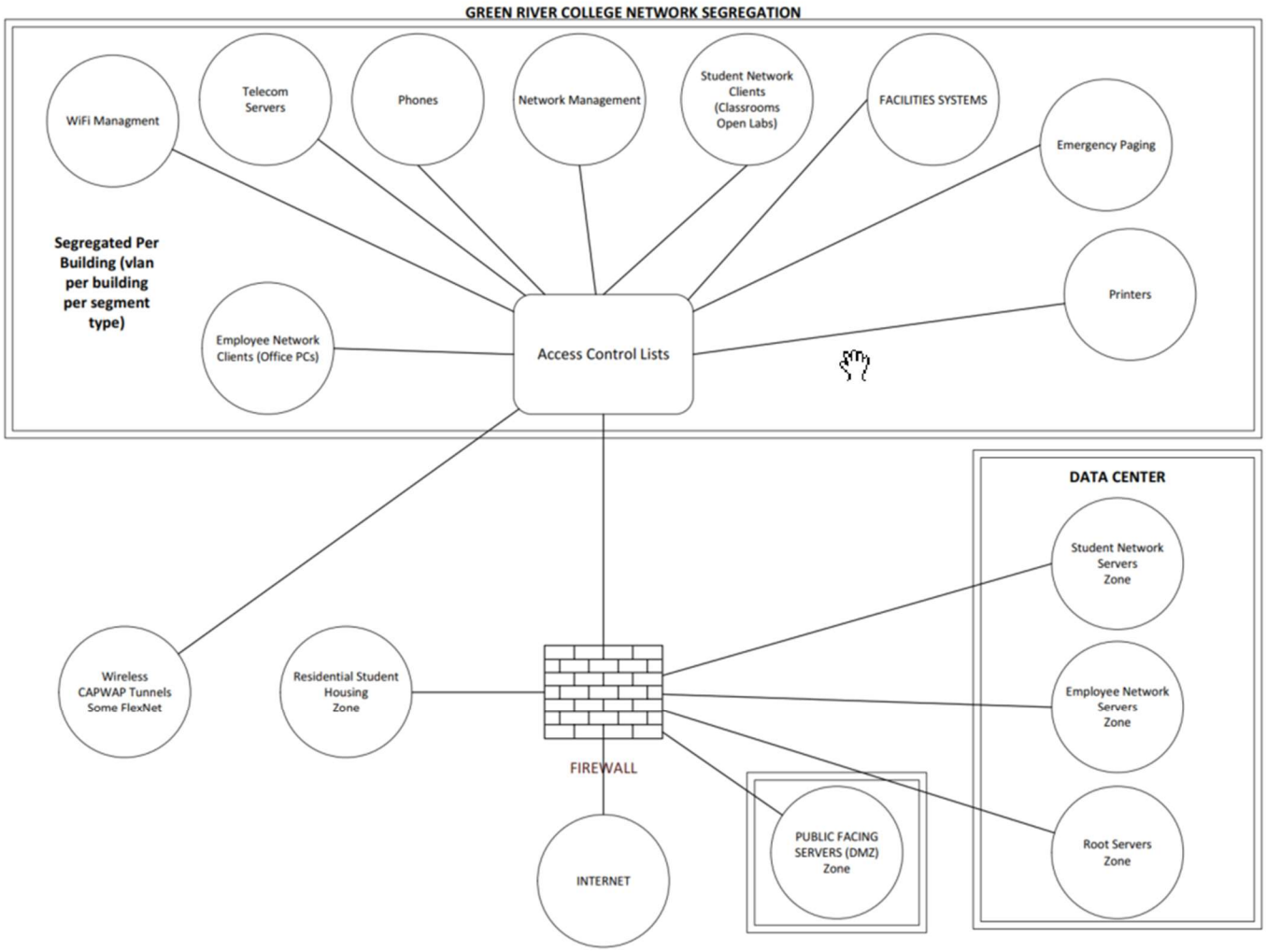
GRC must ensure the secure operation of network assets through the use of appropriate layered protections commensurate with the risk and complexity of the environment.

5.1. Secure Segmentation

Network Infrastructure Security

Green River College is not within the SGN; however, the network infrastructure management process is detailed below.

The following diagram illustrates the logical segregation of Green River College's campus network. Each bubble represents a separate, designated network:



See **Appendix 5.1** for a Master Network Map.

Router access lists are employed to segregate traffic between networks within Green River College's LAN. The basic strategy which governs the placement of workstations within the network is as follows:

Emergency Paging	Speakers, amps, and paging equipment used for emergency notifications.
Employee Network Clients	Employee Network Clients are PCs in offices controlled by lock and key or card key access and are used as office PCs by faculty and staff.
Facilities Systems	Systems used for building controls (e.g., HVAC, power management, lighting, and irrigation). Only has access to facilities servers.
Telecom Servers	Servers, media gateways, session border controllers. Only access to phones and SIP traffic allowed from employee client networks.

WiFi Management	Access Points and Wireless Controllers. Only access to specific servers required to provide network services (DHCP, DNS, RADIUS, Captive Portals)
Network Management	Management interface of routers, switches, other network equipment, and network monitoring devices.
Phones	Voice over IP phones and phone servers.
Printers	Network jacks used by printers (which have DHCP reservations) and only allowed access to print servers which do not use DHCP.
Residential Housing	Student Housing "ResNet" is separated from all GRC networks and uses a separate internet provider, and separate wired and wireless devices.
Student Network Clients	Student Network Clients are PCs in public spaces such as the library, open labs, public classrooms, kiosks, and public areas. These represent the lowest level of access to network resources.
Wireless	Wireless clients are only given access to public facing websites and the internet.
Student Servers (FW Zone)	Student domain servers, file servers, application servers. Student domain workstations have access. Access to other zones limited to specific services.
Employee Servers (FW Zone)	Employee domain servers, file servers, application servers. Employee domain workstations have access. Access to other zones limited to specific services.
Root Servers (FW Zone)	Root domain servers, file servers, application servers. Used as a management domain. Access to other zones limited to specific services. Employee and Student workstations have access to specific servers and services within the Root zone.

Intranet Data Transmission Protection

Separation of the networks described above into different access domains limits the possibility of intercepting data transmissions. Networks are divided according to security needs and physical locations. Segregation of servers from workstations further limits the possibility of intercepting data as it is transmitted between servers.

WAN Data Transmission Protection

Green River College's remote campuses (Auburn, Enumclaw, & Kent) are connected to the main campus LAN over point-to-point links that do not traverse the open internet.

Access Authorization

Access to telecommunications equipment, internetworking servers and networking equipment is limited to those authorized by the Executive Director of Information Technology and is typically limited to Enterprise Services staff.

Access Mechanism Standards

The following common standards are applied to all internetworking servers and equipment:

- Access must be controlled at minimum by username and password combinations. IP based authorization protocols (e.g. Rlogin, NFS, etc.) are not permitted except in cases where traffic can be confined to trusted servers by router access lists or firewalls.
- Where technically feasible encrypted sessions such as SSH are used.

5.1.1 Network Devices

5.1.1.a Network Configuration

As described in the "Network Infrastructure Security" section, internet application services are all contained in an identified external network. Access to services in the Administrative Databases network is limited by router access control list. Enterprise Services must approve network configuration changes. Wherever it is technically feasible, web applications are deployed in multi-tier configurations, protecting higher tier components with network access controls.

5.1.1.b Web Browser/Server Configuration and Use

Web servers are a common entry point for network attacks. To prevent a security breach, Green River College has developed policies and best practices around web server configuration. All users setting up or administering a web server available outside our firewall will read and comply with these policies and practices. Web browsers are identified, deployed, and kept patched by the Enterprise Services team. Only GRC deployed browsers are permitted on GRC equipment.

5.1.1.c Policies and Best Practices Applicable to all Web Servers

1. In general, web users should not be able to log onto a web server locally, via SSH, terminal server, or a console session. This access should only be opened to trained administrators from inside the Green River College firewall.
2. The anonymous user account/context should be configured for the least possible privilege on the system.
3. Web server administration tools must run over different ports than the web content, and they should not be exposed outside of the firewall. A best effort will be made to password protect and encrypt web administration interfaces. Updating content should be password protected even for public access websites.
4. No web server should allow both anonymous upload and download of the same content.
5. Access to a web server through the Green River College firewall will be limited to only the necessary IP addresses and ports.
6. Extraneous services not related to serving web content should be eliminated from the web server.
7. Some web server software installs default content and applications. These should be removed if they are not being used.
8. Web servers and their host operating systems will be promptly patched for security vulnerabilities.

9. Web servers and applications that run on the web servers should be running supported versions and should be kept patched for security vulnerabilities.
10. Web server applications should not be able to execute shell commands and other OS commands that take arbitrary host commands or arbitrary arguments.
11. All web server administrators and web application developers are required to know and understand the security program as it pertains to their position function.
12. Non-public data exposed via a web server presented outside of our firewall must be proxied by another server or device.
13. Exceptions to the recommended policies and best practices can be made with the approval of the enterprise services team after a review.

5.1.1.d Additional Security Requirements for Sensitive/Confidential Data

1. Confidential data needs to be password protected and encrypted during transmission.
2. Authentication to access protected data will be secure and encrypted.
3. An Enterprise Services approved certificate authority must issue SSL/TLS certificates.
4. Data presented via a web server requires the same level of authentication and authorization as locally accessed data.

5.1.1.e Networked Workstation Protection

The following general practices are used to protect workstations from Internet threats:

- Private IP addressing using a continuously recycling network address translation pool.
- Firewall configured to prevent inbound connections

5.1.1.f Virus/Malware Protection and Removal

Information Technology has developed the following practices in support of virus/malware prevention, detection and removal:

- Anti-virus/malware protection measures are deployed on all workstations.
- Anti-virus/malware software is deployed on all Windows servers
- Daily software and DAT file updates are automated on servers and workstations.
- Upon detection of a virus or malware not trapped by anti-viral/malware software a response-team is formed to provide immediate response to all infected users on the LAN.
- If a virus or malware is found on Green River College's network, or threat of infection of a newly released virus/malware is high, users are notified via e-mail of the increased threat.
- The Green River College email gateway blocks all files that cannot be scanned for viruses/malware due to encrypted or password protected content. Specific point-to-point exceptions are allowed based on demonstrated business need.

GRC uses Microsoft's Endpoint Protection (MEP) which has products for communication endpoint, encryption, network security, email security and mobile security as well as unified threat management.

See **Appendix 5.1.1.f** for information regarding the current Anti-Virus and Malware processes deployed to CTR.

5.1.2 Firewalls

Higher Education Exemption

As an institution of higher education, Green River College operates firewall and Internet application services independently from the Washington State Digital Government framework. Specifically, the following practices are intentionally avoided:

- Use of Transact
- Use of Fortress
- Standards for Digital Government Application Submittal

5.1.2.a Firewall Configuration

Green River College maintains a demilitarized zone (DMZ) for Internet applications, and only opens specific TCP ports for each Internet application. For example, for a web application that requires HTTPS access, port 443 and only port 443 is open to that application. Expansion of specific ports surrounding administrative applications is examined on a case-by-case basis by security trained network staff.

5.1.2.b Assessment of User Base

As a regional educational institution, most of Green River College's business practices are centered on communicating with and facilitating business processes with a commuting student body. There is very little overlap between these populations and those served by the digital government.

5.1.2.c Internet Application Submittal Practices

As Green River College's network is outside of the Digital Government framework and resides outside of the firewalls that protect it, we have developed our own practices governing the introduction of new Internet applications. These practices are designed to facilitate academic exploration of web technologies, while providing appropriate protection from related threats.

As deployment of Internet Applications always require configuration of the Firewall, Enterprise Services is always consulted in the deployment of Internet applications (including web servers). Enterprise Services staff uses this consultative process to ensure that:

- The petitioner has adequately evaluated the risk associated with the application.
- Account authentication and authorization techniques are in place for sensitive information.

- If end-user authentication to the application or service is required, that the authentication mechanism is encrypted.
- A system administrator is assigned to ensure that the system is secured appropriately for the application and routinely monitored.

5.1.3 Device Administration

5.1.3.a Network Devices

See **Appendix 5.1.3.a** for a list of network devices

5.1.3.b Windows Server Setup and Configuration

See **Appendix 5.1.3.b** for information regarding the current Windows server setup and configuration processes.

5.1.3.c Linux Server Setup and Configuration

See **Appendix 5.1.3.c** for information regarding the current Linux server setup and configuration processes.

5.1.3.d Network Devices Basic Setup and Configuration

See **Appendix 5.1.3.d** for information regarding the current network devices basic setup and configuration processes.

5.2 Restricted Services

1) GRC provides network services to the public, faculty, staff, and student residents using a variety of access services. The college, as an institution of higher education, has an interest in promoting academic freedom and exploration. The college has developed its own policies, practices, and controls regarding restricted services to meet the college's business requirements.
2) Dial-in and dial-out workstation modems. The college supports some dial-up connections for specific business purposes. Purchase of IT equipment and services (including modems) are reviewed and approved by the Executive Director of Information Technology. Most office phone lines on campus don't support dial-up capabilities without special configuration.
3) Peer-to-Peer sharing applications. The college uses a tool to perform policy enforcement and bandwidth “fair-sharing” on network traffic. Peer-to-peer applications are severely bandwidth constrained discouraging this as a viable practice. All common peer-to-peer applications are additionally blocked on the college’s firewalls.
4) Tunneling software designed to bypass firewalls and security controls. The college doesn't control outbound tunneling software. There are many legitimate uses on campus making controls difficult or impossible. Inbound tunnels are blocked at the firewall unless specifically configured for an approved business purpose.
5) Auto-launching apps. The college doesn't currently prohibit auto-launching applications.
6) Publicly managed e-mail, chat services and video. The college doesn't prohibit these types of services.

7) Products that provide remote control of IT services. The college doesn't currently prohibit or control products that provide remote control of IT services.
8) Information system audit tools. The college doesn't prohibit system audit tools. The college's network security limits the scope of audit tools that might be initiated by a student or the public.

5.3 External Connections

As an institution of higher education, Green River College operates firewall and Internet application services independently from the Washington State Digital Government framework.

5.4 Wireless Connections

5.4.1 Wireless Infrastructure

No wireless access devices are deployed that extend access to administrative networks except in limited cases where there is an overwhelming business need and client access devices are strictly controlled. These networks are required to be both authenticated and encrypted using industry standard authentication, authorization and encryption protocols. Authorization and encryption protocols must be pre-approved by Information Technology. Wireless Encryption Protocol (WEP) has significant security vulnerabilities and by itself is not deemed an adequate encryption protocol. The 802.1x standard for wireless security is considered a minimum for access to administrative systems containing sensitive information.

Green River College's wireless network is centrally managed. All communication between access points and controllers is over an encrypted point-to-point tunnel to prevent wireless traffic from intermingling with data on the wired LAN. Packets traveling from the controller into the campus must pass a network access control list. Access from wireless devices is limited to GRC’s public facing websites, required services (e.g., DHCP and DNS), and internet browsing. Access to administrative networks requires staff and faculty to use the college’s public facing remote access solution.

Detection of rogue access points on the Green River College network is managed through the college’s wireless controller and management system. Data on the presence of rouge access points is continuously collected through all campus AP devices. When rogue devices are discovered to be connected to GRC wired infrastructure, they are disabled at the network level. The exception to this is the Resnet (student housing) network, which has no access to any internal GRC networks, and uses a separate ISP. Students are allowed to plug in personal rogue access points to housing data jacks if they wish.

5.5 Security Patch Management

Deployed software should be reviewed at a minimum of once each academic year. At the time of review, all deployed software at GRC must be running a version that is actively supported by its vendor with only the exceptions noted below allowed. If the deployed version of software at GRC is not supported by its vendor, then it must be upgraded to a supported version as quickly as possible and reviewed to see if it requires remediation while waiting to be upgraded.

If older non-supported software is required for specialized tasks, it must be documented, and any security risks mitigated prior to deployment. For example: Continuing Ed teaching an old version of MS Office that is no longer supported by Microsoft or facilities running control software for EOL (end of life) equipment still deployed on campus. Non-supported software must not be used to access sensitive or confidential data.

Software that requires either non-supported hardware or other software that is not supported (e.g., an old operating system, browser version, or plug-in) to function must be documented, isolated, and upgraded or replaced as soon as possible.

Operating systems and internet browsers must be kept current to within two months of the latest patch release. Operating systems must be within one year of its latest feature update. Operating systems and browsers must be retired and removed from GRC before they reach end of support from their developers.

5.5.1 Patch Management

Windows workstation and server patches are managed through a centrally managed solution. Patches are evaluated and marked for deployment by Enterprise Services staff. Linux server patches are managed with YUM (Yellowdog Updater, Modified) or via vendor patches/updates.

5.5.2 Web Browser and E-mail Client Configuration Practices

Enterprise Services maintains a list of “supported” software applications, which include web browsers and e-mail clients recommended for use. For supported clients, security patches are evaluated and tested by Enterprise Services.

5.5.3 Server Patch Management

Operating system patching has been automated through automated solutions for all of our primary operating systems. With the exception of patches that require direct intervention or designated servers that require dependencies or sequencing of shutdown processes, operating systems are patched automatically during scheduled monthly maintenance windows. OS patch monitoring has been implemented where possible producing alerts for systems out of patch compliance.

Automatic patch monitoring and installation has also been implemented for applications that support this functionality. Green River College has implemented a strategy of selecting solutions wherever possible that facilitates automation of patch management.

For systems where patch monitoring and/or installation automation is not possible, the technical owner of the application, a member of the Information Technology team, takes responsibility for keeping current on new software releases, patches and vulnerabilities and installs updates and patches as appropriate.

In instances where applications are maintained under vendor support agreements, the vendor is responsible for application patching.

5.6 System Vulnerabilities

5.6.1 Web Information Publications

Restrictions governing formal publication review are deemed in conflict of interest with freedom of education and expression at Green River College. As a result, GRC has no formal policy regarding publication of materials to the Internet. Review processes for publication in business offices are left to the discretion of the unit supervisors in coordination with the College Relations Office. The Green River College Appropriate Use of Information Technology Resources policy governs the release of protected and confidential information.

5.7 Protection from Malicious Software

Controls to prevent the introduction of Unauthorized Programs

Enterprise Services has developed the following general practices to prevent introduction of unauthorized programs:

- Virus detection software is deployed on e-mail servers, file servers and client workstations.
- The Internet border is protected with a stateful Firewall.
- General separation of file and web services from application servers (those that execute code).
- Database and application server access limited to system administrators and software developers.
- Separation of academic/administrative web services.

5.8 Mobile Computing

5.8.1 Mobile Computing Security Controls

Laptops, notebooks, and tablet computers have been identified as “small and attractive” and have an increased risk of theft. The following security practices have been developed to guard against these risks:

- Devices are clearly marked as “The Property of Green River College”.
- Each device is assigned a Washington State Identification number or GRC identification number, which is printed on a label affixed to the casing.
- Inventory of this equipment is performed bi-annually.

5.82 Use of Portable Data Storage Devices

- The Green River College, IT-2 Acceptable Employee Use of Technology and Data Policy, prohibits the storage of sensitive data on portable storage devices that have not been approved for use as secure storage devices by GRC.

6. Access Security

6.1.1 Access Management

6.1.1.a Access Authorization

Access to systems containing data classified as having a medium or high risk of disclosure or modification requires the following procedure:

1. User and/or supervisor fill out an account request form.
2. Supervisor identifies the job type to be granted and signs the form.
3. The data guardian identified for the system and/or module verifies the access level and signs the form.
4. Administrative Computing staff verifies that the individual has received FERPA and general operations training necessary for the system involved.
5. Information Technology Staff, in coordination with the data guardian, create accounts and rights as indicated on the form.

6.1.1.b Determining Access Rights

Access rights to forms and data are assigned to specific job types for all systems. The job type indicated on the User Account Request Form is used to assign specific roles, classes and access control lists. The IT Help Desk forwards each request for changes in access granted to a particular job type to the appropriate data guardian for review and approval.

6.1.1.c Specialized Data Access Mechanisms

Green River College's client/server systems utilize advanced application and system level security techniques to ensure that users cannot bypass application logic such as:

- Application-asserted roles
- Password-protected roles.
- Updates and inserts abstracted through stored procedures.
- Value based security around modification of financial data.

6.1.1.e Evaluation for Immediate Action

The Data Guardian and/or Information Technology staff evaluate the risk and liability associated with the incident as appropriate. If the risk or liability to the institution associated with the incident is high and can be mitigated by immediate action, then one or more of the following immediate actions may be considered:

- Disabling of the user's account
- Revoking access to systems or applications.
- Disabling network ports

For example: If it is believed that the act of sharing a password may allow unauthorized modification or disclosure of data that is classified high risk, the users account may be disabled to mitigate the risk to the data.

6.1.1.f User Education

Green River College acknowledges that most violations of security practices can be effectively addressed with user education.

For example: Users are instructed on the personal and institutional risks and liabilities associated with sharing passwords. They are also educated on the institutional password sharing practices.

6.1.1.g Referral

If education is unsuccessful at correcting the behavior, then the incident is documented and referred to the appropriate authority for determination of disciplinary action based on user classification:

Faculty	Academic Deans & Human Resources
Staff	Supervisor or Manager of Employee & Human Resources
Students	Judicial Affairs and Compliance Officer

6.1.2 Accounts

There is no expectation of privacy for any GRC provided account or solution. GRC is a public entity and must respond to all properly made requests for information. Replying to those requests or other legally made inquiries may require providing data from GRC provided accounts or solutions.

6.1.2.a Logon and Password Controls

Users are required to use *hardened passwords* or lengthy passphrases wherever possible.

6.1.2.b Vendor Access

When necessary, vendors are manually issued login accounts. Where possible vendors are issued non-privileged accounts. Privilege escalation mechanisms are audited as well as all domain logons. When necessary, vendor accounts are temporarily enabled with an automatic expiration date.

Vendors are monitored continuously when working on workstations or servers.

6.1.3 Network Access Security

Access to network resources such as web applications, file services and e-mail are controlled by Green River College's instances of AD and Entra ID.

6.1.3.a Issuance

GRC uses an automated tool to provision and deprovision Active Directory accounts and emails for both students and employees. Other accounts (domain admin, service, contractor, etc.) are created and managed manually.

Employee network and email accounts are automatically issued (with the network account in a disabled state) two weeks before the user's employment start date (as found in ctcLink) and enabled on their employment start date.

Most student network and email accounts are automatically issued (with the network account in a disabled state) upon registration for a class. Student network accounts are enabled the day the class they are registered for begins.

International Programs (IP) student network and email accounts are automatically issued (with the network account in a disabled state) upon detection that their "Acceptance Letter" was sent. IP student network accounts are enabled on the day the class they are registered for begins and disabled again three weeks after they stop attending classes (unless they are registered for another class).

Student email accounts are initially assigned email only licenses. The student's email account license is upgraded to the full license on the day the class they are registered for begins. Unless they are registered for another class, three weeks after they stop attending classes, the student's license is reduced to email only again and they have 30 days of read-only access to any other content (e.g. OneDrive files) they have created so that they can move it to personal data storage. Their email account will remain licensed as email-only until they begin taking another class or their account is deleted.

Contractor accounts are issued with an expiration date set to the planned end of engagement wherever technically possible. In cases where this is not possible the project technical lead maintains responsibility for revoking account access.

All active users are assigned a unique account name.

Student accounts are assigned to the "@student.greenriver.edu" domain and their account names are generated automatically with the following naming convention: <LastName>.<FirstName> or if that would be a duplicate account name, then: <LastName>.<FirstName>.<#>, and if there is no first name, then simply <LastName> or if that would be a dupe: <LastName>.<#>. Example: the first student

named: “John Doe” would have a username of: “Doe.John” and the second student named: “John Doe” would have a username of: “Doe.John.2”.

Employee accounts are assigned to the “@greenriver.edu” domain and their account names are generated automatically with the following naming convention: <FirstName>.<LastName> or if that would be a duplicate account name, then: <FirstName>.<LastName>.<#>, and if there is no first name, then simply <LastName> or if that would be a dupe: <LastName>.<#>. Example: the first employee named: “John Doe” would have a username of: “John.Doe” and the second employee named: “John Doe” would have a username of: “John.Doe.2”.

6.1.3.b Revocation

Unless HR puts a hold on their account, employee accounts are disabled upon their employment termination date (per ctclink) and deleted three weeks later. HR notifies IT if an employee’s data (H drive or e-mail) should be retained temporarily, or if another employee should be given access to it.

Most student network and email accounts are deleted one year after they stop attending classes if they are not registered for another class.

IP student network and email accounts are deleted three years after they stop attending classes if they are not registered for another class. IP student network and email accounts are also deleted two years after their “Acceptance Letter” was sent if they never actually register for a class.

6.1.3.c Suspension and Renewal

Employee network accounts are disabled upon their employment termination date (per ctclink).

Student network accounts are disabled three weeks after they stop attending classes (unless they are registered for another class) and renewed if they register for another class prior to their account being deleted.

Under rare circumstances such as disciplinary action or long-term leave, accounts may be disabled. Security violations or suspected compromised accounts may cause suspension of the account as approved by the Executive Director of Information Technology. All systems administrators and technical support staff are instructed to only re-enable accounts that have been manually disabled after consultation with the Executive Director of Information Technology or the Information Security Officer.

6.1.4.c Session Inactivation

All employee desktop images (including remote access) are configured to lock after 15 minutes of inactivity. Student desktop images are prevented from locking due to the determination that it would be disruptive if students were able to intentionally or inadvertently cause a computer to lock, thus

preventing the use of that computer by another student until some form of manual intervention was taken (e.g., a local administrator forcibly closing the session or the computer being forcibly rebooted).

6.2 Password Requirements

6.2.1 Hardened Passwords

Green River College has implemented a password scheme that will work across its operating systems, internetworking servers, client/server and mainframe platforms. Where feasible, passwords conform to the following general scheme based off of the current NIST recommendations and, where appropriate, PCI-DSS requirements:

- Passwords must be a minimum of 12 characters.
- Users are instructed to not use only a single word that can be found in a dictionary, but can include multiple words in a passphrase
- Users are instructed to never write down passwords, or store them in any non-encrypted electronic password vault solution
- Passwords must not contain:
    - Username
    - UserID
    - Any form of the user's full name
    - More than three sequential characters (e.g., 1234, or abcd)
    - All repetitive characters (e.g., aaaaaaa)
    - Known compromised or common passwords
    - Context-sensitive passwords (e.g., Gre3nR!ver)
- Passwords must be significantly different from the previous 7 passwords. Passwords that increment (Password1, Password2, Password3 ...) are not considered significantly different
- All vendor default passwords must be changed before solutions are placed into production
- All initial or administratively reset passwords must be changed on first login

These constraints are technically enforced, although the specific rule enforcement may vary on systems that have technical limitations (e.g., that disallow certain special characters). The primary password set mechanism in our Active Directory and our password reset solution enforce the above rules as much as possible.

The annual IT security awareness training includes information regarding the proper handling of passwords and password hardening.

6.2.2 Multi-Factor Authentication

GRC requires MFA for all employees and students.

6.2.3 Student Information System Security Practices

Green River College uses the instance of PeopleSoft managed by the SBCTC (called “ctcLink”) as the enterprise-wide administrative system. The SBCTC sets and manages login and password policies for ctcLink This section describes the basic practices surrounding ctcLink security.

All users require a ctcLink logon for initial access to the system and by default are only granted access to basic self-service applications. Additional permissions to GRC sensitive data is granted as necessary and only after the data steward has granted permission for that user to have access to that specific data and the user has completed the appropriate training.

A user’s ctcLink username is their EMPLID. The SBCTC manages password requirements, password reset options, and MFA requirements. Users are required to set their own password upon activating their ctcLink account.

Permissions to GRC sensitive data in ctcLink are revoked when a user separates from the college.

6.2.4 Logons and Password Controls

All usernames and passwords are managed by the IT Enterprise Services team and where technologically possible follow a combination of the current WaTech, NIST and PCI-DSS guidelines for password length, complexity, and aging. Where technically possible, accounts are locked out after a maximum of 5 failed attempts for a period of 30 minutes and then re-enabled automatically. Office 365 logons lock after 3 failed attempts for a period of 30 minutes and then re-enable automatically, and idle user logon sessions are locked after 15 minutes.

When necessary, employees must use the GRC deployed self-service password reset tool to reset their employee Active Directory account’s password. If they have not configured their password reset Q&A profile or have forgotten the proper responses to their Q&A profile, then their supervisor must approve a password reset request for them via the IT Helpdesk.

When necessary, students must use the GRC deployed self-service password reset tool to reset their student Active Directory account’s password using their pre-populated Q&A profile. On first login, students configure a password reset option (text, email, etc.) with Microsoft to be able to reset their GRC email account. If they are unable to use the Microsoft option, then they authenticate themselves on the GRC website and request a manual password reset to be processed by GRC IT staff.

6.3 Authentication

Green River College uses Microsoft’s Active Directory as its primary authentication database. The system supports a wide variety of protocols for authentication. Green River College leverages Active Directory for authentication via native MS protocols, LDAP, RADIUS and ADFS for web-based single sign-on. All

authentication requests are secured through mechanisms native to the protocol in use such as Kerberos or via SSL/TLS for layered protocols such as LDAP.

User Lock and Active Directory auditing is in use for all login attempts against Active Directory. Systems such as ctcLink that have their own authentication system employ auditing built-in to the system and auditing of logins is enabled everywhere that it is available.

6.4 Remote Access

6.4.1 Dial up Lines and Networking

No dial-up lines are used to facilitate access to client/server systems. Green River College does not provide dial-up networking.

6.4.2 VPN Solutions

Green River College is not connected to the SGN, however it operates limited VPN's within the campus network to facilitate secure connections for third party vendor interfaces, some IT administrative tasks, and the connection of various state or SBCTC solutions. The following general strategies are used to ensure VPN's do not constitute risk.

- Firewall restrictions limit VPN connectivity to established, trusted networks, and cannot be accessed from the general network.
- VPN settings are done using hardware VPN devices (not client software) configured by network staff.
- VPN configurations are password protected; only authorized, trained IT support staff are given the passwords to alter VPN configurations.
- Split firewall configurations are not employed.

6.4.3 Vendor Access

Facilities vendors are granted access on rare occasions to perform contracted repairs, upgrades, and configurations. On those occasions, the vendor is set up as a temporary user with the minimum allowed privileges and granted access either locally or via a secure remote access connection. As soon as the work is completed, the user account is disabled, and remote access is removed. On-going direct access is never granted to vendors.

ctcLink and its exported data has several machine interfaces for data exchange with third parties. These interfaces process transactions through mid-tier interface programs that validate the data and generate audit information for all transactions. Data is protected in transit via PGP, TLS, or SFTP.

6.4.4 Application Access

Employees and students have access to protected applications through Azure Virtual Desktop (AVD). All sessions are encrypted using an AVD-proprietary algorithm. Access to the AVD service is controlled by GRC network accounts and is limited to employees or students as appropriate.

Students also have access to protected applications through Quest vWorkspace. All sessions are encrypted using a Quest-proprietary algorithm. Access to the vWorkspace service is controlled by GRC network accounts and is limited to students.

6.4.5 Internet Remote Access

Remote access to file services and e-mail services is facilitated primarily through web applications and ADFS. They are authenticated using GRC network accounts through Office 365. All sessions are encrypted using SSL (HTTPS) encryption.

Devices used to access the GRC remote access solution should be fully patched (within 1 month) and running current (within 1 week) anti-virus/anti-malware solutions.

7. Application Security

7.1 Planning and Analysis

7.1.1 Data Entry Processes

The following business practices have been adopted to ensure integrity of data entry tasks.

- Auditing of all data entry tasks for data identified as having a high risk of modification.
- Separation of responsibility for data entry and authorization for high risk data (e.g. financial/purchasing transactions.)
- Written requests from data guardians required for programmatic modification of data identified as having a medium or high risk of data modification.

7.1.2 Processing Accuracy

In areas where risk of data modification is high such as financial modules, the following practices have been developed to assure data processing accuracy:

- Each morning the amounts recorded in the Financial Management System are balanced with the posted internet credit card transactions. Any discrepancies are immediately investigated and resolved.
- Each month the Business Office balances the banking records, including all internet transactions, with the Financial Management System.

7.2 Application Development

7.2.1 General Internet Application Practices

This section describes the general practices around applications that govern most of the colleges Internet applications. Although many of Green River College's web applications are exempt from these

standards, the following guidelines are used for the configuration of all web services except in cases where following them would cause a significant impact to teaching, learning or research activities at the institution.

Program source code is located in secured file shares. The file shares are secured via Active Directory security groups. Only individuals with a business need are allowed access to program source code.

Currently, GRC does not contract for outsourced software development.

7.2.2 Software Development Practices

1) Separate development, test, and production environments. The college has separate environments for its mission-critical software applications.
2) Implement separation of duties or other security controls between development, test and production environments. The controls must reduce the risk of unauthorized activity or changes to production systems or data including but not limited to the data accessible by a single individual. The college uses an agile deployment method. At a minimum code is reviewed and approved by team leads before being deployed into production. Major code upgrades or deployments are reviewed and approved via the change control process.
3) Production data used for development testing must not compromise privacy or confidentiality. Prohibit the use of Category 3 data or higher in development environments unless specifically authorized by the GRC IT Security Program Plan. Production data in any environment must meet or exceed the level of protection required by its data classification. The college uses production data in development and test environments to aid in code development and testing. The test and development environments use the same access and security controls as the production environment.
4) Removal of test data and accounts before production systems become live.
5) Removal of customer application accounts, usernames, and passwords from production environments before applications become active or are released to customers.
6) Review of custom code prior to release to production or customers to identify potential coding vulnerabilities as described in Section 7.4
7) Appropriate placement of data and applications in the IT infrastructure based on the risk and complexity of the system.
8) Use of appropriate authentication levels.

7.2.3. Procedures to Prevent Common Coding Vulnerabilities

1) GRC will develop software and applications based on secure coding guidelines. An example is the Open Web Application Security Project guidelines which includes:

   a. Un-validated input.
   b. Weak or broken access control such as malicious use of User IDs.

c. Broken authentication/session management such as use of account credentials and session cookies.
d. Cross-site scripting (XSS) attacks.
e. Buffer overflows.
f. Injection flaws such as SQL injection.
g. Improper error handling that creates other conditions, divulges system architecture or configuration information.
h. Insecure storage.
i. Denial of service.
j. Insecure configuration management.

2) Review code to detect and mitigate code vulnerabilities that may have security implications when significant changes have been made to the application.

7.2.4 Risk Assessment

Projects classified as high risk of disclosure, medium risk of modification or medium risk of disruption are referred to the Information Security Officer and Executive Director of IT for approval.

7.2.5 Selecting Identity Confidence

The following strategies are used in determining the mechanisms required or recommended for protecting Internet applications:

Public	Information may be published to the web without the need to understand who may see it. No identity confidence mechanisms are required.
Community	Information does not contain any “protected” information, but due to its “preliminary nature”, it is desired to limit the exposure of the material to a smaller group of individuals. Applications should protect information with a username and password.
Confidential	Data is protected information and access must be authorized on an individual basis. Username and passwords must be protected.

7.2.6 Authentication Mechanisms

Wherever it is technically possible Green River College has secured web applications using ADFS. This service uses Kerberos authentication to authenticate user identity against GRC’s Active Directory domain. ADFS never exposes the actual credential to the application and secures all communication in a channel directly between the user and the authentication service. Applications only receive

authentication validation directly from the ADFS service, never from user input. This allows the application to leverage existing policies and practices regarding issuance, revocation, suspension and renewal.

7.2.7 Issuance, Revocation and suspension

Wherever it is technically possible issuance and revocation is governed by section 0 covering issuance and revocation of network accounts.

7.2.8 Protection Mechanism

Users and developers of applications are required to use TLS 1.2 or later encryption for all web authentication mechanisms. Web applications that exchange sensitive data must use TLS 1.2 or later encryption for the entire session.

7.2.9 SSL Certificates

All of Green River Colleges SSL certificates are purchased through well-established commercial providers and are fully compatible with current versions of mainstream web browser software.

7.3 Application Maintenance

7.3.1 Software Version Control and Testing

Green River College uses the following version control practices for systems that store data that have medium or greater risk of disclosure, modification or disruption:

- All code is tested in pre-production environments by end users, or by IT personnel in cooperation with end users.
- Peer review is performed prior to introducing developed code into production.
- Developers and system administrators are required to log any upgrades and new development performed on systems to shared electronic log.
- Developers and end user testers are instructed to perform positive and negative testing as described in shared test plans for each system or module.

7.4 Vulnerability Prevention

The college will prevent common coding vulnerabilities in software development processes. The college will:

(1) Develop software and applications based on secure coding guidelines.

(2) Review code to detect and mitigate code vulnerabilities that may have security implications when significant changes have been made to the application.

See **Appendix 7.4** for information regarding the coding vulnerability monitoring configuration and information processes.

7.5 Application Service Providers

The college's current practice is to assess applications hosted by a service provider and incorporate security language appropriate to the sensitivity of the data into the vendor agreement.

8. Operations Management

8.1 Change Management

Green River College has implemented a manual network management process to backup, archive and track changes to network device configurations. The process also includes getting alerts when patches are available. Patch application includes a rollback path. All changes are logged to a centralized store to include what changed, why the change was made and the business need it serves. Access to view and modify network configurations is strictly controlled and limited to Enterprise Services staff.

8.1.2 Distribution and Destruction of Output Reports

Green River College does not operate an “operations center” responsible for the distribution of reports to other agencies or work units. Authorized users print reports directly in their work areas.

The supervisor of each work area is responsible for establishing data security practices for their group. Common practices for handling report production and disposal:

- Reports containing sensitive information are hand delivered by staff to other divisions or departments.
- Document shredders and/or secure shred bins are distributed in each of the work areas that manage sensitive data. Users are instructed to shred all personally identifiable data.

Electronic data or reports containing sensitive data for inter-departmental use are stored in secured network file shares. Electronic data or reports transmitted to external agencies is encrypted.

8.2 Asset Management

8.2.1 Information Asset Overview

This section is designed to provide an overview of Green River College’s information assets. Green River College’s information assets fall into the following categories:

Health Data	Green River College operates a small-scale Counseling Center that maintains medical records of students. This data requires a high degree of protection from data disclosure and modification.

Enrollment Data	Enrollment Services maintains pre-admissions student directory information, student directory information, enrollment data and student transcript data. This data requires a high degree of protection from disclosure and modification.
Employment Data	Much of the salary and employment data housed in payroll and human resource systems is a matter of public record. However, social security numbers, benefits information, home addresses and phone numbers do qualify as protected information. This data requires a high degree of protection from disclosure.
Financial Aid Data	The office of Financial Aid maintains information in support of application for and disbursement of student grants, loans and scholarships. This includes educational, demographic and tax information including social security numbers, student and parent income, aid eligibility, awards and disbursements. This data requires high degree of protection from disclosure and modification.
Financial Data	Purchasing, accounts receivables, general ledger and bank statements. This data requires a high degree of protection from modification.
Campus Safety Data	Incident and case files typically associated with law enforcement. This data requires a high degree of protection from data disclosure and modification.

8.2.2 Governing Regulations

HIPAA	The Health Insurance Portability and Accountability Act (HIPAA) defines the Federal Privacy requirements for health care data.
RCW 70.02	Washington State interpretation and application of HIPAA governing health care data.
FERPA	The Family Education Rights and Privacy Act protects the privacy associated with student educational records. Data includes student demographics, enrollment, financial aid, and grievance data.
Higher Education Act	The Higher Education Act governs most aspects of the disbursement of financial aid. Checks be issued within ten days of receiving awards. Prolonged disruption of financial aid systems carries potential legal and fiscal liabilities.
Gramm-Leach-Bliley Act	Governs protection of information for consumers of financial services. This includes Financial Aid loans and collections. Mandates the establishment and on-going maintenance of an IT Security Plan to protect consumer information.
The Patriot Act	Governs release of data under specific cases where a subpoena or search warrant is issued for student information, requiring us to maintain confidentiality of such requests.
PCI-DSS	The Payment Card Industry – Data Security Standard governs how credit card data is protected.

8.2.3 Information Asset Oversight

The institution has identified Data Guardians for each of the information assets.

Information Asset	**Assigned Guardian**
Student pre-enrollment, enrollment, and transcript data	Registrar
Student Health Records	Dean of Instruction for English and Humanities
Network identity/directory information	Executive Director of Information Technology
Financial Aid Records	Director of Student Financial Aid
Campus Safety and Parking	Director of Campus Safety and Transportation
Circulation Systems	Dean of Library, E-Learning and Media Services
Human Resources Data	Vice President for Business Administration and Human Resources
Finance, Accounting and Grants	Vice President for Business Administration and Human Resources
Housing Data	CCA Director of Housing and Residence Life

Each Data Guardian is responsible for overseeing access to and maintenance of the indicated assets, including:

- Training and awareness programs for users with access to sensitive information.
- Authorizing access to view and/or modify data.
- Reviewing and revising respective Data Security Policy Statements.
- Reviewing the Security Program for accuracy

8.2.4 Inventory of IT Assets

Tagged IT equipment that is located at a specific user's desk is tracked as part of the general asset management of the college and assigned to that user. Shared desks have equipment assigned to the appropriate generic user e.g., "Shared Faculty". Major IT equipment like servers and network gear in the server rooms or network closets is tagged as part of the general asset management of the college, is assigned to the "IT Department" with responsibilities assigned to the Executive Director of Information Technology.

8.3 Media Handling and Disposal/Data and Program Backup

8.3.1 Enterprise Backup Policies

Green River College runs a centralized enterprise backup solution to guarantee data security. The basic characteristics of the system are:

1. The primary media are HDD-based storage devices, which employ de-duplication and compression located on campus that then replicates all changed blocks to a secure, off-site, online, hosted storage solution.
2. Centralized monitoring and reporting of backups and restores.
3. Encrypted backup/restores and storage of backups.
4. Policy based retention of backups.
5. Policy based scheduling of backups.
6. Policy applied based on system risk analysis.
7. 24-hour availability of vendor-support.
8. Automated management and tracking of primary and off-site copies and off-site storage.

Internet traffic logs are not part of the enterprise backup solution but are collected and stored by the firewall device. Data from the firewall is archived for a year on a separate HDD based repository.

The retention of data (files, web, database, server, etc.) via the enterprise backup solution is for 30 days. Data on a single server can be archived in the same manner with a single storage policy, or divided between different storage policies. Frequency of backups is based upon the data type. Presently, there are three data retention storage policies:

Storage Policy	Data Covered	Description
Internet Logs	All internet logs as captured by the firewall.	Backups captured daily by the firewall and then archived for a year to a separate HDD-based storage repository.
File-Web-Databases	File shares, websites, and databases servers that store business critical data.	Backups captured daily with primary and replicated copies retained for 90 days.
Semi-Static	Application servers and servers that contain data that does not change frequently and does not require long-term archiving. Backups are for disaster/program recovery.	Backups captured every other week with primary and replicated copies retained for 90 days.

In general, each storage policy requires that at a predetermined number of valid restore points exist before “pruning” any old data out of our system.

Backups are automated with “schedule policies” determined by the nature of the data and the recovery modes necessary.

Continuous replication is used for all policies requiring off-site storage.

8.3.2 Backup Media

- Initial backup targets are housed in secure facilities managed by Enterprise Services.
- Physical access to backup targets is limited to Enterprise Services staff and tightly controlled.
- Replicated backup targets are hosted in the cloud in secure locations by vendors that contract to high levels of security and tightly controlled access to their systems.

8.3.3 Media Disposal

The college has a contract with a secure destruction vendor to securely destroy and dispose of media on an ad hoc basis. All media used by Enterprise Services in a secure computer operations area is securely destroyed when it is time to be retired.

8.3.4 Telephony Backup

Daily backups to disk are performed automatically by the enterprise backup solution for the legacy PBX system.

The new MS Teams based VOIP telephony system is not backed up beyond the standard resiliency provided by a cloud hosted solution.

8.3.5 Voice mail Backup

Daily backups to disk are performed automatically by the enterprise backup solution for the legacy PBX voice mail system.

Copies of voice mails in the new MS Teams based VOIP telephony system are sent to the user's email inbox which automatically includes them in the email journaling mailbox.

8.3.6 Transporting Data beyond GRC Boundaries

Any media containing information protected against unauthorized access, misuse, or corruption beyond GRC campus boundaries is not allowed.

9. Electronic Commerce

9.1 E-Commerce Strategy

Green River College does not perform any E-Commerce development.

Green River College uses a third-party vendor, Elavon, to process e-commerce transactions for payments on student accounts and other miscellaneous fees. Typical charges paid on student accounts include tuition, parking fees, library fees, etc. Typical miscellaneous payments (generally made by non-students) include admission fees, and event registrations.

Green River College has chosen to outsource e-commerce in the following areas:

- The college accepts payments on student accounts and other related fees via a hosted service provided by Elavon.
- The college bookstore E-commerce site is a hosted service provided by MBS Store Technology Solutions.

Outsourcing of financial transactions is subject to approval and review of the Vice President for Business Administration. The Vice President for Business Administration ensures that a review has been performed by Enterprise Services for appropriate transaction security prior to implementation.

All credit card processing at GRC is performed by systems designed and qualified for presence on and traversal of the public Internet.

10. Security Monitoring and Logging

10.1 Processing Audit Trails

Applications have been selected for their ability to perform the following types of logging:

- All data modifications are recorded to include user and time stamp.
- Domain controllers record all successful and failed domain authentication events.

Application audit logs are reviewed by Enterprise Services staff in response to system problems or internal audit requests.

In general log files are secured on servers with access provided only to authorized individuals

10.2 Time Source Synchronization

All systems are synced with an NTP time source.

10.3 System Access Violations

Enterprise Services is responsible for system log analysis in support of detecting and preventing system access violations. Enterprise Services is also responsible for developing preventative measures to protect systems from potential security breaches.

Typically, access violations are either reported to Enterprise Services or discovered in periodic monitoring of systems. Enterprise Services staff triage the problem and decide on an appropriate course of action depending on the nature of the access violation, which may include but is not be limited to:

- Shutdown of services for patching and/or repairs
- Temporary disabling of accounts
- Implementing additional audit mechanisms or surveillance equipment

11. Incident Response

Green River College is not connected to the State Governmental Network and does not participate in WACIRC or WaTech CSIRT. All computer incidents are reported to Green River College Information Technology. Incidents are logged and when appropriate an ad-hoc incident response team will be formed to analyze the situation and determine a response plan.

See Appendix 11 for documents pertaining to the Incident Response Plan

All GRC employees are accountable for their own actions. It is each employee's responsibility to be able to identify scams such as email phishing attempts and avoid them. If an employee suspects that their, or another GRC account has been compromised or that there has been a breach of GRC data or computing

resources, then they are responsible for notifying the appropriate campus resources (IT, Campus Safety, HR, Student Affairs, etc.) so that an incident response process can be initiated.

11.1 Intrusion Detection

Network Services is responsible for performing routine intrusion detection tasks and has developed the following practices in support of intrusion detection and follow-up:

- Vendor Vulnerability Reports, SANS NewsBites, and other professional lists are monitored to gain awareness of periods of increased threat level.
- Protocol classification software is deployed as part of the Internet border firewall to facilitate weekly monitoring of traffic trends for anomalies.
- Packet inspection, antivirus, anti-spyware, vulnerability protection, URL blocking of malicious sites, URL blocking of newly created domains, and DOS protection is performed at the Internet firewall.
- Antivirus signatures, threat databases, and application threats are updated at least every 24 hours. URL database is updated every 5 minutes.
- DNS blackholing is performed to prevent access to malicious sites and botnet control.
- Rogue Detection scans for unauthorized wireless access points.
- Threat log reports are sent and reviewed daily, including protocol and application distribution analysis.

Frequency is at minimum once per quarter but increases in direct relation to advertised increase of threat levels for the campus.

11.2 Last Test of Incident Response Plan

See the Executive Director of Information Technology or Information Security Officer or designee for information pertaining to the last test of the Incident Response Plan.

Appendix Documents List

Appendix 1.3.a – Significant Infrastructure Projects

- Teams > IT Security > General > IT Security Program Appendix Documents > Significant Infrastructure Projects.xlsx

Appendix 1.7.c - Compliance Activities Pending-Completed

- Teams > IT Security > General > IT Security Program Appendix Documents > Compliance Activities Pending-Completed.xlsx

Appendix 2.c – Acceptable Use of Technology and Data Policy

- https://www.greenriver.edu/campus/policies-and-procedures/information-technology-policies/it-2-employee-acceptable-use-of-technology.html

Appendix 2.2 - IT Security Awareness Training and Information

- Teams > IT Security > General > IT Security Program Appendix Documents > IT Security Awareness Training and Information.docx

Appendix 2.10 - Contractors

- Teams > IT Security > General > IT Security Program Appendix Documents > Contractors.xlsx

Appendix 2.11 - Separations

- Teams > IT Security > General > IT Security Program Appendix Documents > Separations.xlsx

Appendix 5.1 - Master Network Map

- Teams > IT Security > General > IT Security Program Appendix Documents > Network Core Physical Topology.vsdx

Appendix 5.1.1.f – Anti-Virus/Malware Configuration and Information

- Teams > IT Security > General > IT Security Program Appendix Documents > Anti-Virus-Malware Configuration and Information.docx

Appendix 5.1.3.a - Network Devices

- Teams > IT Security > General > IT Security Program Appendix Documents > Network Devices.xlsx

Appendix 5.1.3.b - Windows Server Setup and Configuration

- Teams > IT Security > General > IT Security Program Appendix Documents > Windows Server Setup and Configuration.docx

Appendix 5.1.3.c - LINUX Server Setup and Configuration

- Teams > IT Security > General > IT Security Program Appendix Documents > LINUX Server Setup and Configuration.docx

Appendix 5.1.3.d – Network Devices Basic Setup and Configuration

- Teams > IT Security > General > IT Security Program Appendix Documents > Network Devices Basic Setup and Configuraton.docx

Appendix 7.4 - Coding Vulnerability Monitoring Configuration and Information

- Teams > IT Security > General > IT Security Program Appendix Documents > Coding Vulnerability Monitoring Configuration and Information.docx

Appendix 11 - Incident Response Plan

- Teams > IT Security > General > IT Security Program Appendix Documents > Incident Response Plan.docx
- Teams > IT Security > General > IT Security Program Appendix Documents > Incident Response Flowchart.pdf
- Teams > IT Security > General > IT Security Program Appendix Documents > Incident Response Form.docx