

Worcester State College Information Technologies’ Business Practices Guide

Draft 2.01

Contents

1. Security Vision and Policy Overview.....	7
1.1 Summary.....	7
1.2 Introduction.....	7
1.2.1 Scope.....	8
1.2.2 Threats.....	8
1.3 Authority.....	8
1.4 Change Control.....	8
1.5 Other Management Responsibilities.....	9
1.5.1 General Management.....	9
1.5.2 Data Security Officer.....	9
1.5.3 Data Security Administrator.....	9
1.5.4 System Administrators.....	10
1.6 Deviations, Waivers, and Exceptions.....	11
1.7 Reporting of Suspected Violations.....	11
2. E-Business and Partner Security Policy.....	12
2.1 Policy Statement.....	12
2.2 Applicability.....	12
2.3 Justification.....	12
2.4 Minimum Implementation Standards.....	13
2.4.1 Information Valuation.....	13
2.4.2 Network Connectivity.....	13
2.4.3 Protection Solution for E-Business and Business Partners.....	13
2.5 Compliance.....	14
3. Appropriate Use of E-Mail and Telecom Resources.....	15
3.1 Policy Statement.....	15
3.2 Applicability.....	15
3.3 Justification.....	15
3.4 Minimum Implementation Standards.....	15
3.4.1 Information Protection Responsibilities.....	15
3.4.2 Privacy.....	16
3.4.3 E-Mail.....	16
3.4.4 Computer System and Network Resources.....	16
3.4.5 System and Network Use Warning Notice.....	16
3.4.6 Modems.....	17
3.4.7 Reporting Suspected Security Violations.....	17
3.5 Compliance.....	17
4. Anti-Virus Policy.....	18
4.1 Policy Statement.....	18
4.2 Applicability.....	18
4.3 Justification.....	18
4.4 Minimum Implementation Standards.....	18
4.4.1 Monitoring.....	18
4.4.2 Anti-Virus Configuration and Scanning.....	19
4.4.3 Reporting.....	19

4.4.4 User Installed Software	19
4.5 Compliance	19
5. System Administration Security Policy	20
5.1 Policy Statement	20
5.2 Applicability	20
5.3 Justification.....	20
5.4 Minimum Implementation Standards.....	20
5.4.1 Documentation	20
5.4.2 Configuration Management.....	21
5.4.3 Asset Protection	21
5.4.4 Log/Monitor/Audit.....	21
5.4.6 Incident Response	22
5.4.7 Policy Enforcement.....	22
5.5 Compliance	22
6. Personnel Security Policy	23
6.1 Policy Statement	23
6.2 Applicability	23
6.3 Justification.....	23
6.4 Minimum Implementation Standards.....	23
6.4.1 Specific Position Security Requirements	23
6.4.3 User Responsibilities.....	24
6.4.4 Data Owner Responsibilities	24
6.4.5 Employee and Contractor Transfer, Extended Leave, and Termination	24
6.4.6 User Security Training	24
6.4.7 Disciplinary Practice	24
6.5 Compliance	25
7. Privacy Policy.....	26
7.1 Policy Statement	26
7.2 Applicability	26
7.3 Justification.....	26
7.4 Minimum Implementation Standards.....	26
7.4.1 General.....	26
7.4.2 Worcester State Privacy Principles	26
7.4.3 “Common Sense” Security Practices	27
7.4.4 Records Retention and Disposal	27
7.4.5 Social Security Numbers (SSN) and Personal Identifiers	27
7.4.6 Business Relationships	28
7.4.7 Cookies	28
7.4.8 Marketing Data	28
7.4.9 Data accuracy.....	29
7.5 Compliance	30
8. Information Valuation and Protection Policy	31
8.1 Policy Statement	31
8.2 Applicability	31
8.3 Justification.....	31
8.4 Minimum Implementation Standards.....	31
8.4.1 Information Valuation and Categorization Guidelines.....	31
8.4.2 Storage	33
8.4.3 Transmission	33
8.4.4 Information Protection	33
8.4.5 Information Marking/Labeling.....	33
8.5 Compliance	33
9. Computer and Network Security Policy	34
9.1 Policy Statement	34

9.2	Applicability	34
9.3	Justification	34
9.4	Minimum Implementation Standards	34
9.4.1	Access Management	34
9.4.2	Account Management	34
9.4.3	Information Transmission	35
9.4.4	Monitoring	35
9.4.5	Reporting of Suspected Violations	35
9.5	Moves, Adds, and Changes	35
9.6	Escalation	36
9.7	Compliance	36
10.	Internet and WWW Security Policy	37
10.1	Policy Statement	37
10.2	Applicability	37
10.3	Justification	37
10.4	Minimum Implementation Standards	37
10.4.1	Access Control	37
10.4.2	Protection of Network and Computing Resources	37
10.4.3	Web Browsing and General Internet Access	38
10.5	Compliance	38
11.	Password and PIN Security Policy	39
11.1	Policy Statement	39
11.2	Applicability	39
11.3	Justification	39
11.4	Minimum Implementation Standards	39
11.4.1	Password/PIN Confidentiality	39
11.4.2	Password/PIN Length	39
11.4.3	Password Complexity	39
11.4.4	Password/PIN Expiration	40
11.4.5	Default Passwords/PINs	40
11.4.6	Password/PIN Reuse	40
11.4.7	Password/PIN Changes	40
11.4.8	Password/PIN Delivery	40
11.4.9	Emergency Delivery of a One-Time Password	41
11.4.10	Policy Enforcement	41
11.5	Compliance	41
12.	Account Management Security Policy	42
12.1	Policy Statement	42
12.2	Applicability	42
12.3	Justification	42
12.4	Minimum Implementation Standards	42
12.4.1	New Accounts	42
12.4.2	Unused Accounts	42
12.4.3	Failed Login Attempts	42
12.4.4	Policy Enforcement	42
12.5	Compliance	43
13.	Remote Access Security Policy	44
13.1	Policy Statement	44
13.2	Applicability	44
13.3	Justification	44
13.4	Minimum Implementation Standards	44
13.4.1	Centralized Access	44
13.4.2	Authentication	44
13.4.3	Management Authorization	45

13.4.4	Protection of Worcester State Information and Computing Resources	45
13.4.5	Remote Access by Non-Worcester State Employees	45
13.4.6	Session Management and Audit	45
13.4.7	Diagnostic Access	46
14.	Vendor/Consultant Access Security Policy	47
14.1	Policy Statement	47
14.2	Applicability	47
14.3	Justification	47
14.4	Minimum Implementation Standards.....	47
14.4.1	Security Policy Compliance	47
14.4.2	Sponsor Responsibilities	48
14.5	Compliance	48
15.	Access Control Gateway Security Policy	49
15.1	Policy Statement	49
15.2	Applicability	49
15.3	Justification	49
15.4	Minimum Implementation Standards.....	49
15.4.1	General	49
15.4.2	Periodic Assessment.....	49
15.4.3	Access Control	50
15.4.4	Configuration	50
15.4.5	Logging and Auditing	50
15.4.6	Administration	51
15.5	Compliance	51
16.	Portable Computer Device Security Policy	52
16.1	Policy Statement	52
16.2	Applicability	52
16.3	Justification	52
16.4	Minimum Implementation Standards.....	52
16.4.1	Protection of Access.....	52
16.4.2	Protection of Data	52
16.4.3	Equipment Identification.....	53
16.4.4	Report Losses	53
16.5	Compliance	53
17.	Encryption Policy	54
17.1	Policy Statement	54
17.2	Applicability	54
17.3	Justification	54
17.4	Minimum Implementation Standards.....	54
17.4.1	Employment	54
17.4.2	Encryption Process.....	54
17.5	Compliance	54
18.	System and Application Development Security Policy	55
18.1	Policy Statement	55
18.2	Applicability	55
18.3	Justification	55
18.4	Minimum Implementation Standards.....	55
18.4.1	Security Requirements Analysis and Specifications	55
18.4.2	Security Verification and Validation.....	55
18.4.3	Custom Developed Software and Testing	56
18.4.4	Unauthorized Installed Software	56
18.4.5	Commercial Off-the-Shelf Software	56
18.4.6	Copyright Law	56
18.4.7	Continuity of Service	56

18.5 Compliance	56
19. Incident Reporting and Response Policy	57
19.1 Policy Statement	57
19.2 Applicability	57
19.3 Justification	57
19.4 Minimum Implementation Standards	57
19.4.1 Incident Reporting and Escalation	57
19.4.2 Internal Incident Response Team	57
19.4.3 External Incident Response Team	58
19.4.4 Incident Response Process	58
19.4.5 Computer Investigations and Evidence	58
19.5 Compliance	58
20. Intrusion Detection Policy	59
20.1 Policy Statement	59
20.2 Applicability	59
20.3 Justification	59
20.4 Minimum Implementation Standards	59
20.4.1 Intrusion Detection Technology	59
20.4.2 Deployment	59
20.4.3 Configuration	59
20.4.4 Data Management	60
20.4.5 Incident Response	60
20.5 Compliance	60
21. Information System Asset Control Policy	61
21.1 Policy Statement	61
21.2 Applicability	61
21.3 Justification	61
21.4 Minimum Implementation Standards	61
21.4.1 General	61
21.4.2 Employment	61
21.4.3 Loss of Enterprise Assets	61
21.4.4 Enforcement	62
21.5 Compliance	62
22. Configuration Management Policy	63
22.1 Policy Statement	63
22.2 Applicability	63
22.3 Justification	63
22.4 Minimum Implementation Standards	63
22.4.1 General	63
22.4.2 Documentation	63
22.4.3 Software Updates and Patches	63
22.4.4 Standard Software Configurations	64
22.4.5 Software Other Than Standard	64
22.5 Compliance	64
23. Government Regulation Compliance Policy	65
23.1 Policy Statement	65
23.2 Applicability	65
23.3 Justification	65
23.4 Minimum Implementation Standards	65
23.4.1 Protection Solution(s)	65
23.5 Compliance	65
24. Continuity of Operations and Disaster Recovery	66
24.1 Policy Statement	66
24.2 Applicability	66

24.3 Justification	66
24.4 Minimum Implementation Standards	66
24.4.1 General	66
24.4.2 Prioritization	66
24.4.3 Prevention	66
24.4.4 Roles and Responsibilities	67
24.4.5 Documentation	67
24.4.6 Data Backup	67
24.4.7 Safety	67
24.4.8 Security	67
24.4.9 Test Plan	68
24.4.10 Update Plan	68
24.5 Compliance	68

1. Security Vision and Policy Overview

1.1 Summary

Worcester State College recognizes that information is a critical business asset and that its ability to manage, control, and protect this asset will have a direct and significant impact on its future success.

Information should be considered in the broadest sense to include research, intellectual property, business, and course development, marketing, and strategic plans, student, faculty, employee, and business partner information, finance, human resources, consulting, partnerships, and contracts. Information can be in the form of audio, video, paper, magnetic, and electronic form.

Business information must be protected from theft, loss, destruction, unauthorized alteration and unauthorized access. The compromise or loss of business information can have an adverse impact on competitive position and growth, the ability to comply with laws and regulations, and the integrity and trust inherent in the Worcester State name.

Worcester State's inherent use of interconnections with business partners, suppliers, students and faculty, along with the direct use of the Internet, have combined to make the management, control, and protection of information more complex and difficult. Worcester State Information Assets are to be appropriately protected at all times. All faculty and staff shall ensure that all Worcester State Information Assets under their control are protected. The college must:

- Identify and value its most critical information assets;
- Assess the risk that these assets might be lost/stolen, altered, destroyed, or made unavailable;
- Implement appropriate management controls and processes to ensure the continued productivity of these assets in producing business results.

Violations of this policy may be grounds for disciplinary action, including dismissal. This document establishes the policies for information security to ensure that the enterprise can efficiently and effectively manage, control, and protect its business information assets and those information assets entrusted to Worcester State by its students, faculty, employees, and business partners.

1.2 Introduction

These policies for *Worcester State College's Division of Information Technologies* were developed to ensure an adequate and consistent approach to the management, control, and protection of business information assets across all Worcester State data. These policies allow for the application of more robust methods for special business needs, and provide for exceptions, if they do not place the enterprise or other operating units in an unacceptable risk posture.

1.2.1 Scope

These policies are comprehensive in scope and apply to the full Worcester State information asset space. Worcester State Information Assets include all confidential or proprietary information, Worcester State intellectual property (including, but not limited to, inventions, patents, know-how, design, copyrights, and trade secrets), and all data or information whose unauthorized destruction, alteration, or disclosure outside the College could result in any of the following:

- • Impact on the integrity or public trust in the Worcester State name
- • Financial loss
- • Loss of competitive position
- • Degraded business operation
- • Violation of a Worcester State information protection agreement with another party
- • Failure to comply with legal or regulatory requirements

1.2.2 Threats

These policies address the full spectrum of threats to the business from active threats such as hackers, competitors, and disgruntled employees, to passive threats such as hardware, software failures, operator errors, power, and communication outages.

1.3 Authority

The Worcester State Chief Information Officer (CIO) is the Authority for the Security Policy, and all other Worcester State policies, processes, and procedures referenced from this document. Any addition, removal, or modification to this document or any Worcester State documents referenced herein must be made in accordance with the Change Control process defined in the next segment of this section. Management positions other than the Security Policy Authority may be cited as being responsible for the implementation of some specific components within policies, processes, and procedures, but in all cases those responsibilities are subject to the review and control of the Security Policy Authority. Any failure to comply with requirements specified within this document or its referenced policies, processes, or procedures will be evaluated by the Security Policy Authority for appropriate action.

1.4 Change Control

Any proposed change to the Security Policy, or other related policy, process, or procedure that uses this document, as a reference must be submitted to a Worcester State Data Security Officer for review. The Data Security Officer will evaluate the need for the change, its potential impact on Worcester State, and provide a recommendation to the CIO as to whether the change should be approved. The CIO will make the final decision on all approval requests. When a change is approved, all other documents in the Worcester State policy structure affected by the change will be reviewed, under direction of the CIO, to ensure the changes are applied to other documents where appropriate. A revised version of the Security Policy should be published and disseminated to all employees, contractors, and consultants annually or whenever there are significant policy changes, and each should be required to sign a revised policy acknowledgment form.

1.5 Other Management Responsibilities

1.5.1 General Management

The IT Technical Leader for Worcester State is responsible for the planning, implementation, and compliance with these policies. Protection plans and procedures shall, as appropriate, address the following:

- A framework and responsible person to initiate, implement, and manage an ongoing information security program;
- Limiting or controlling access to Worcester State Information Assets by both Worcester State employees and non-Worcester State personnel;
- Minimizing the intentional or unintentional loss, theft, destruction, corruption, or misuse of Worcester State Information Assets by Worcester State employees, non-Worcester State personnel, or due to acts of Nature;
- Continuing of business operations should Worcester State Information Assets be destroyed, altered, or compromised;
- A mandatory education and awareness program for all employees.

1.5.2 Data Security Officer

A Data Security Officer must be identified within the College, to lead the information security program. The Data Security Officer will:

- Develop and lead the implementation of a comprehensive Information Security Program for the College;
- Be the primary spokesman for the security needs of the business as changes in technology, business strategy, and threat occur;
- Represent the College's business security interests in the establishment of policies, practices, standards, and procedures;
- Ensure the unique information security needs of the business are addressed;
- Establish and oversee a process that ensures information security is an integral part of the business planning and execution;
- Ensure the overall program is kept current with changing business needs and risks;
- Perform risk assessments and security reviews;
- Assist management with security risk management decisions.

1.5.3 Data Security Administrator

A Data Security Administrator will be identified as necessary to support the Data Security Officer.

The Data Security Administrator will report to the Data Security Officer or the CIO. The Data Security Administrator will:

- Monitor the behavior of the systems or servers under their control;
- Support the Internal Security Incident Response Team;
- In the absence of a Data Security Administrator, the Data Security Officer will fulfill these responsibilities.

1.5.4 System Administrators

In addition to acknowledgement of security policies that apply to the general user, system and network administrators should sign a compliance agreement indicating that they have read and understand the College's policies and procedures that apply specifically to their administration duties.

Administrators should maintain tables, diagrams and other records of baseline system and security configuration, and any configuration changes for all hardware and software system components under their administration. Documentation requirements may include:

- Security configuration for operating systems, client/server, legacy and standalone applications, infrastructure equipment (router, switches, premise), and security servers (firewall, intrusion detection, authentication server, etc.).
- Contact information (name, address, phone, pager, e-mail, service/product/expertise, etc.) for all individuals and organizations that may contribute to system support. This includes system administrators, managers, communications service providers, expert consultants, maintenance and technical support contractors and equipment and software vendors.
- Special information, such as student ID number, PIN, circuit and port numbers, account number, etc., that may be needed when contacting support personnel.
- Passwords for all administration related accounts and systems. These passwords must be stored and maintained by a local security authority.
- LAN/WAN architecture diagrams with references to physical locations.
- Server operating system services (e.g. domain controllers, WINS, DNS, DHCP, print, file, remote administration, etc.) and how and where they are installed.
- Application software services (e.g. messaging, database, web, tape backup, security, etc.) and how and where they are installed.
- Router configurations, routing tables, and Access Control Lists (ACL).
- Switch configuration.
- Operating System configuration(s) (e.g. Solaris, Windows NT).
- Firewall configuration.
- Mail Server configuration.
- Web Server configuration.
- Premise equipment configuration.
- Location of vendor manuals (hardcopy and electronic) for all hardware and software components.
- Hardware inventory with type, model, purpose, and location.
- Software inventory with version, patch level, installation options, purpose, location, license numbers, and keys.
- Rack inventory.

1.6 Deviations, Waivers, and Exceptions

Any deviations, waivers, or exceptions to these policies must be submitted in writing to the CIO, or designee of the CIO. Worcester State organizational units may add local information security policies to meet unique business, environmental, or legal needs, provided they are more stringent than, and do not diminish, the policies.

1.7 Reporting of Suspected Violations

All employees, consultants, and contractors must report any suspected violation of these policies to their Data Security Officer. All reports of alleged violations of this policy will be investigated on a case-by-case basis. Access privileges may be suspended during the course of the investigation. Violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

2. E-Business and Partner Security Policy

2.1 Policy Statement

Worcester State business interactions and electronic Business (e-Business) connections with its business partners must be appropriately protected to ensure confidentiality, integrity, authenticity, and availability of all Worcester State and business partner information.

2.2 Applicability

This policy applies to all members of the Worcester State College community.

2.3 Justification

New and expanded business relationships with other companies, vendors, and consultants are necessary for the continued growth of Worcester State. The level of access granted and information shared with business partners may vary greatly. The type and value of information exchanged between Worcester State and its business partners will vary. Such information could include personnel information, pricing, marketing information, vendor/supplier information, research data, and special process or technology descriptions. The protection of such information during transmission and while stored on Worcester State or partner information systems must meet the protection requirements of the information owner. Before information is released to, or exchanged with, a business partner, the information owner must determine the value of the information. This must be the basis for the selection of appropriate protection.

In addition to growth projections and bottom-line business value, e-Business is about transforming the way businesses operate and interact with customers and partners. As Worcester State increasingly externalizes its businesses to the world, there is a requirement for effective security. An effective solution must minimize the risk of business data being lost or modified and ensure that applications remain available while performing as intended.

2.4 Minimum Implementation Standards

2.4.1 Information Valuation

In establishing a relationship with a business partner, an initial risk assessment must be made to determine the value of the information exchanged and system access shared and the acceptable level of risk to Worcester State.

The capability of the business partner to properly protect Worcester State proprietary or confidential information during transmission, processing, and storage must be assessed before such information is released to the partner through any available media. Worcester State must ensure that the level of protection provided for information obtained from a business partner is equal to or greater than the protection required by the business partner for its information. In cases where the business partner has more stringent protection requirements, Worcester State must implement the protective measures or receive a written waiver from the business partner.

Business partner relationships must be periodically reassessed to determine the value of the information exchanged and system access shared remain at an acceptable level of risk to Worcester State.

2.4.2 Network Connectivity

When connecting a business partner's network or systems to the Worcester State network, the security of the connecting network must be evaluated prior to making the connection.

2.4.3 Protection Solution for E-Business and Business Partners

Based on the assessment of each business partner and the establishment of an acceptable level of risk, a protection solution, which includes these principles, as appropriate, must be designed to achieve the acceptable level of risk. To adequately protect the relationships between Worcester State and any business partner, the following criteria must be considered in the design of the required protection solution:

- **Accountability:** Capability to determine who performed any given action and which actions occurred during a specific time interval. Ability to identify who did what, when.
- **Administration:** Capability to define, maintain, monitor, and modify business partner information. This information can be customized and updated as required.
- **Assurance:** Capability to demonstrate and periodically validate that the claimed level of security protection is being enforced. Confirmation that the system carries out policy rules.
- **Authorization:** Capability to allow access to facilities, systems, data applications, or networks to legitimate business partners only.
- **Authenticity:** Capability to provide for reliable identification of business partners. When data is exchanged, provide assurance of data origin and prevent business partners from denying having participated in a transaction.
- **Availability:** Capability to keep systems, data networks, and applications usable. Ensure systems and network resources are available to support business partner interactions.
- **Confidentiality:** Protection from unauthorized disclosure of data.

- **Integrity:** Capability to protect business transactions from unauthorized and undetected modification.

Additionally, e-Business and Business Partner connections must have the following attributes:

- Security solutions must be based on an integrated, standards-based architecture
- Only Worcester State standard security components may be used in developing security solutions
- All parties to these connections must have clearly stated security and information access requirement policies
- Ask for necessary information only
- Release information only when necessary, and then only the minimum information necessary for the stated purpose

2.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

3. Appropriate Use of E-Mail and Telecom Resources

3.1 Policy Statement

All Worcester State networking and computing resources must be used predominately for business purposes.

3.2 Applicability

This policy applies to all members of the Worcester State College community.

3.3 Justification

Worcester State provides networking and computing resources to its employees, contractors, consultants, and other Worcester State authorized parties (hereafter known as “Users”) for their use in performing their job requirements. Networking and computing resources include, but are not limited to, electronic mail (e-mail), voice mail, video conferencing, facsimile, telephone, Internet services, computer hardware and software, network hardware or software, printers and copiers, and other printed or electronic media. The college permits users to utilize these networking and computing resources in imaginative and innovative ways, provided the use benefits Worcester State or its employees, in general, and does not involve personal gain or activities contrary to Worcester State’s credo or policies.

3.4 Minimum Implementation Standards

3.4.1 Information Protection Responsibilities

Worcester State’s information protection responsibilities are:

- All users must be responsible for protecting critical business information assets.
- Users must follow the access and handling requirements identified in the information security policies.
- Users are responsible for safeguarding and monitoring information assets against unauthorized disclosure, modification, and destruction.
- Users must ensure that all remote access service provides sufficient privacy for the value and category of the information being accessed.
- Users must ensure that precautions are taken to protect Worcester State networking and computing resources and business information when uploading software, files, and data from the Internet or sources other than those controlled by Worcester State.
- Only Worcester State approved remote devices may be used for remote access to services.
- The use of personal or non-Worcester State issued remote devices requires the approval of the Data Security Officer, and an agreement with the user that the device will be maintained in accordance with all policies.
- Dual use of computers for both personal and business functions must be used predominately for business purposes.
- All Worcester State owned or controlled information, software, and hardware must be returned upon a user’s end of employment.
- Remote access via the Internet must be protected with strong authentication.

3.4.2 Privacy

All messages sent, received, or stored using Worcester State computers, and information processing equipment, or sent over any Worcester State network are college property and there should not be any expectation of privacy. Worcester State reserves the right to filter content that may be accessed via enterprise Internet connections and the use of enterprise messaging systems does not include an expectation of privacy. Worcester State employees are required to respect the privacy of all employees and organizations using the Internet, and must not intentionally seek personal information belonging to Internet users or other employees.

3.4.3 E-Mail

The conduct of Worcester State business is the primary purpose of college messaging systems. Limited appropriate personal use is permitted when it does not interfere with normal work activities. Use of electronic messaging systems for transmission or distribution of inappropriate or offensive material, such as racial or gender slur, pornographic, sexually explicit, or non-business-related materials such as chain letters, is strictly prohibited. Users of Worcester State electronic messaging systems must not misrepresent themselves or Worcester State in any communications, nor at any time may a Worcester State employee make derogatory comments against any competitor. At no time may proprietary or confidential critical business information be transferred using the electronic messaging systems without the use of approved protection mechanisms (e.g. encryption).

3.4.4 Computer System and Network Resources

Networking and computing resources include, but are not limited to, e-mail, voice mail, video conferencing, facsimile, telephone, Internet services, computer hardware and software, network hardware or software, printers and copiers, and other printed or electronic media.

3.4.5 System and Network Use Warning Notice

Use of any Worcester State computer system constitutes consent to monitoring at all times. All Worcester State computer systems and related equipment are intended for the communication, transmission, processing, and storage of Worcester State information only. All Worcester State computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems, to prevent unauthorized use and violations of security policies and applicable laws, to deter criminal activity, and for other similar purposes. Worcester State computer systems must have warning notices prior to and after login. Any user of a Worcester State computer system should be aware that any information placed in the system is subject to monitoring and review by data system administration, security, or management personnel. Worcester State policies and standard business operations provide for no expectation of privacy for employees, contractors, or consultants using Worcester State computers or networks.

If monitoring of any Worcester State computer system, or review of data residing on any Worcester State system, reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of any Worcester State computer systems reveals violations of security policy or unauthorized use, employees who violate security policies or make unauthorized use of Worcester State computer systems are subject to appropriate disciplinary action, which may include termination of employment.

3.4.6 Modems

Desktop personal computers (PC) connected to the Worcester State network are prohibited from having direct modem connections or Integrated Switch Digital Network (ISDN) terminal adapters and must go through a secure remote access. Laptop PCs equipped with a modem must be used predominately for business purposes while on Worcester State College premises. Laptop PCs equipped with a modem will not be connected to the Worcester State enterprise network without prior approval from the Data Security Officer.

3.4.7 Reporting Suspected Security Violations

Users must report any suspected violation of any information security policy to their Data Security Officer.

3.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

4. Anti-Virus Policy

4.1 Policy Statement

Worcester State networking and computing resources must be protected from malicious software codes and viruses.

4.2 Applicability

This policy applies to all members of the Worcester State College community.

4.3 Justification

Malicious software codes and viruses can cause data loss, degradation of system and network performance, and create significant demands on Information Technology (IT) support resources.

4.4 Minimum Implementation Standards

4.4.1 Monitoring

Worcester State reserves the right to monitor the content and traffic patterns and/or electronically screen networking and computing resources, including activity, and traffic originating remotely. Purposes for such monitoring, and/or screening include, but are not limited to, system maintenance, detection, and elimination of contamination, detection and prevention of unauthorized disclosures of Worcester State confidential or proprietary information, detection of unauthorized access to computing and network resources, and determination of compliance with Worcester State policies.

Worcester State reserves the right to intercept and/or quarantine any networking or computing resources that may pose a threat to Worcester State, including, but not limited to, data, messages, network traffic. If such monitoring, screening, interception, and/or quarantine reveal possible evidence of criminal activity, Worcester State may provide the evidence of such monitoring to law enforcement officials.

4.4.2 Anti-Virus Configuration and Scanning

All Worcester State computer systems must have current, approved Anti-Virus software installed, properly configured and running at all times (never disabled). The Anti-Virus software must be configured to automatically clean the infected file (remove the virus) or to quarantine the infected file if automatic cleaning is not possible. Scans must occur without user intervention, and on systems where this is not possible, user are responsible for initiating the scan on desktop systems, laptop systems and single user workstations; and the system administrator is responsible for servers. In each case, the user or system administrator is accountable for ensuring that the scans are performed in accordance with this policy.

Electronic mail must be scanned “in transit” when it enters or leaves the Worcester State enterprise network (i.e., to/from the Internet or to/from a business partner). All desktop and laptop systems, e-mail/collaboration/groupware servers, and file-and-print servers must be configured to automatically perform an anti-virus scan on both local and hosted drives, upon startup and weekly.

4.4.3 Reporting

Users and/or data system administrators must immediately notify the Data Security Administrator whenever a computer virus is suspected or detected.

4.4.4 User Installed Software

Worcester State licenses the computer software it uses from a variety of affiliated and unaffiliated companies. Worcester State does not own this software, but purchases a license in order to be able to use it. Any unauthorized reproduction or copying of such software, whether for business or personal use, is prohibited. All software may be used only in accordance with the terms of the license agreement. If you are unsure if any action may violate such a license agreement, request authorization from your Data Security Officer before proceeding. Misuse of software, equipment, or resources will subject the employee to disciplinary action up to and including termination.

4.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

5. System Administration Security Policy

5.1 Policy Statement

Worcester State data system administration security practices must ensure that all Worcester State information systems are in a known, secure state and information resources are protected.

5.2 Applicability

This policy applies to all members of the Worcester State College community.

5.3 Justification

Long-term security effectiveness relies heavily on conscientious security administration. System security will degrade over time unless knowledgeable personnel are dedicated to its maintenance. Administrators must be ever vigilant to maintain systems in a secure state.

5.4 Minimum Implementation Standards

5.4.1 Documentation

Administrators must maintain tables, diagrams and other records of baseline system and security configuration, and any configuration changes for all hardware and software system components. All information listed below must be maintained in multiple, protected, locations to guarantee its availability when needed, while preventing its disclosure to all but authorized personnel.

Documentation requirements may include:

- Security configuration for operating systems, client/server, legacy and standalone applications, infrastructure equipment (router, switch, premise), and security servers (firewall, PKI, intrusion detection, authentication server, etc.).
- Contact information (name, address, phone, pager, e-mail, service/product/expertise, etc.) for all employees and organizations that may contribute to system support. This includes data system administrators, managers, communications service providers, expert consultants, maintenance and technical support contractors and equipment and software vendors.
- Special information; such as student identification (ID) number; Personal Identification Number (PIN); circuit, port, and account numbers, etc., that may be needed when contacting support personnel.

5.4.2 Configuration Management

Security configuration must be consistent with Worcester State standards where they exist. Administrators must regularly monitor applicable vendor sources for information regarding security bulletins or the release of security software patches. Administrators must apply all system and security patches (service packs, hot fixes, patch clusters, etc.) after they have been locally tested and approved, and document the baseline configuration.

Documentation must include the equipment/software affected, the patches applied, their version, their purpose, where they were obtained, installation procedure, and any subsequent configuration. If a patch or patches cannot or should not be applied, a written rationale must be provided to the CIO, or equivalent position. Administrators must regularly monitor Internet and other information sources for security advisories that pertain to constituent system products (e.g., www.microsoft.com/security).

5.4.3 Asset Protection

Administrators must ensure that anti-virus software is installed and updated in accordance with the Anti-Virus Policy. Administrators must grant users only the privileges necessary to perform their duties (least privilege), with respect to configuration of access control restrictions. Physical access to all servers and networking/internetworking premise equipment must be restricted to authorized personnel only.

Administrators must protect password and account information that resides on authentication servers (e.g., a Microsoft Windows NT primary or backup domain controller). Data must be routinely saved to a magnetic tape hardware/software system, or other removable storage medium, to maximize availability and prevent information loss.

5.4.4 Log/Monitor/Audit

Administrators must provide logging functions for system security events related to logon/logoff, creation of accounts, access privileges, user rights, permissions, group membership, unauthorized access attempt, account lockout, security policy and process tracking.

5.4.5 Periodic Maintenance

Administrators must utilize tools and procedures to evaluate configuration and verify functionality and integrity of security services. The tools that are being utilized must be actively supported so that frequent updates are available, and must support both automated and on demand use. Maintenance must be provided on all user accounts, and administrators must disable or delete all inactive accounts.

5.4.6 Incident Response

Administrators must report and respond to security events or suspicious activity in accordance with the Worcester State Incident Reporting and Response Policy.

5.4.7 Policy Enforcement

Administrators must configure and maintain all systems in accordance with Worcester State Information Security Policies.

5.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

6. Personnel Security Policy

6.1 Policy Statement

All Worcester State employees, vendors, business partners, and outside consultants or contractors who require access to critical business information must be appropriately screened, trained, and supervised.

6.2 Applicability

This policy applies to all organizational units, vendors, business partners, contractors, and consultants.

6.3 Justification

Security requirements must be addressed during recruitment, included in job descriptions, and monitored during an employee's employment to reduce the risks of theft, fraud, human error, or the misuse of Worcester State resources.

6.4 Minimum Implementation Standards

6.4.1 Specific Position Security Requirements

Positions requiring access to critical business information must be identified, and all security requirements critical to performance of job responsibilities must be clearly defined in employee's job descriptions.

All Worcester State employees and non-Worcester State personnel, including contractors, who have access to a computer system, which processes or stores Worcester State information must have a background check commensurate with the highest level of information processed by the system. In unusual circumstances, the Worcester State responsible party may make exceptions to this requirement.

6.4.2 Management Responsibilities

All Worcester State managers are responsible for proactively enforcing the information security policies and practices. Senior management must support, maintain, and monitor the effectiveness of, and compliance with, the information security policies and practices.

Information security must be included as an aspect for consideration in an employee's performance review.

6.4.3 User Responsibilities

All Worcester State employees, contractors, consultants, vendors, and business partners must be responsible for protecting critical business information assets. Users must follow the access and handling requirements identified in the information security policies. Users must be held responsible for safeguarding and monitoring information assets against unauthorized disclosure, modification, and destruction.

6.4.4 Data Owner Responsibilities

The Data Owner is responsible for determining the appropriate valuation of information.

- The Data Owner must communicate the information value and handling categorization when the information is released or provided to another entity.
- The Data Owner is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.

Access to critical business information assets must be based upon the minimum privileges necessary for the user to perform duties, need-to-know, and physical access necessary to accomplish assigned responsibilities. Each Data owner must be responsible for determining the value associated with potential loss or damage to critical business information assets and ensuring that a practice is in place to determine and monitor access to critical business information assets under his/her control.

6.4.5 Employee and Contractor Transfer, Extended Leave, and Termination

All employee and contractor transfers, extended leave, and termination of employment notices must be immediately provided to the Data Security Officer. If possible, notification should be made before the event occurs to ensure the appropriate steps can be taken to remove or disable accounts, or revise privileges, as necessary.

6.4.6 User Security Training

Every Worcester State staff member must sign an Information Security Policies and Practices Acknowledgement form stating that he/she has read and understands the enterprise, and local information security policies and practices. A security training and awareness program, including local information security policies and practices, must be part of the orientation for all new employees. All Worcester State staff must receive information security training and awareness briefings at least once a year, and records must be maintained of security training and awareness participation for Worcester State personnel. All Worcester State staff members, contractors, consultants and temporary employees, who have access to critical business and information assets, must be trained in information security control measures and sign an Information Security Policies and Practices Acknowledgement form.

6.4.7 Disciplinary Practice

A formal disciplinary practice for non-compliance with information security policies and practices must be developed in conjunction with human resources and legal counsel. Disciplinary practice must be correct and fair and may involve action up to and including termination for repeat offenders or severe violations. Criminal or civil liability may apply to any employee who violates systems or network security. Non-Worcester State employees who

violate the information protection policies may have their access removed or suspended, their companies notified, or legal action taken. The action taken in any given situation will be decided jointly between the data owner and the Data Security Officer.

6.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

7. Privacy Policy

7.1 Policy Statement

Information about Worcester State, its operations, its students, faculty, and staff obtained in the conduct of Worcester State business is the property of the College and is confidential. Such information must not be disclosed or used for purposes other than the conduct of Worcester State business, as required by law, or as permitted by written Worcester State practice.

7.2 Applicability

This policy applies to all members of the Worcester State College community.

7.3 Justification

At Worcester State, the protection of the privacy of our students, faculty, employees, business partners, vendors, suppliers, and consultants is a primary responsibility.

7.4 Minimum Implementation Standards

7.4.1 General

All Worcester State Web sites must have a privacy policy available for visitor review.

7.4.2 Worcester State Privacy Principles

All developed and deployed Worcester State systems will adhere to these privacy principles:

- **Openness.** There must be a general practice of openness about practices and policies with respect to personal information. Means must be available to establish the existence and nature of personal information and the main purposes of its use.
- **Purpose specification.** The purpose for collecting personal information must be specified at the time of collection. Further uses must be limited to those purposes.
- **Collection limitation.** The collection of personal information must be obtained by lawful and fair means and with the knowledge and consent of the subject. Only that information necessary for the stated purpose will be collected.
- **Use limitation.** Personal information must not be disclosed for secondary purposes except with the consent of the subject or by authority of law.
- **Individual participation.** Individuals must be allowed to inspect and correct their personal information. Whenever possible, personal information will be collected directly from the individual.
- **Quality.** Personal information must be accurate, complete, and timely, and be relevant to the purposes for which it is to be used.
- **Security safeguards.** Reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, or disclosure will protect personal information. Access to personal information must be limited to only those within the organization with a specific and valid need to see it.

- **Accountability.** Someone within the organization, i.e., the Data Security Officer, must be held accountable for complying with its privacy policy. Employee training programs and privacy audits to monitor organizational compliance must be conducted on a regular basis.

7.4.3 “Common Sense” Security Practices

When providing copies of information for others, employees must ensure that nonessential information is removed and that personally identifiable information, which has no relevance to the transaction, is either removed or masked (the process of “redacting” or “severing” the record).

Employees must never leave computer terminals unattended when personally identifiable information is on the screen. Use of password-activated, screen-saver programs on systems that process personal information is mandatory.

All employees who handle personal information—including temporary, back-up and contract staff—must be trained to detect when they are being solicited for personal information by potentially unauthorized and unscrupulous persons. “Pretext” interviews are more common than might be expected and is the stock-in-trade of persons bent on finding out confidential personal information to which they are not entitled.

7.4.4 Records Retention and Disposal

All records retention/disposal must be done in accordance with the classification level of the documents and Worcester State records retention/disposal policy. When disposing of computers, diskettes, magnetic tapes, hard drives, and any other electronic media that contain personally identifiable materials, all data must be completely erased using an approved Worcester State sanitation product, or the hardware must be destroyed.

7.4.5 Social Security Numbers (SSN) and Personal Identifiers

The use of SSNs as personal identifiers and for record-keeping purposes must be strongly discouraged and, preferably, prohibited. Proliferation of SSNs puts students and employees at risk of allowing unscrupulous persons to obtain the number for fraudulent purposes; for example, gaining access to one’s banking and credit accounts.

If the organization must use the SSN as a record-keeping number, it must offer the option of using an alternative number. The display of SSNs on any documents that are widely seen by others is strictly prohibited.

If an access code is required for certain transactions (i.e., ATM cards, security system codes, building access cards, passwords), the use of SSNs, or any part of the SSN such as the last four digits, as personal identifier numbers is prohibited.

7.4.6 Business Relationships

While Worcester State is not responsible for the privacy policies of businesses and Web sites with which business relationships may or will exist, the security measures and privacy practices of such organizations should be examined before entering into a business arrangement. The protection of Worcester State's reputation and public trust, as well as the privacy of its students, faculty, staff, and associates, is an important responsibility.

7.4.7 Cookies

"Cookies" is a technology that can be used to provide tailored information from a Web site. A "cookie" is an element of data that a Web site sends to the users browser, which may then store it on the users system. Worcester State Web sites must be designed to work with users who will accept the download of "cookies" and, except for the purposes of session tracking for secure applications, must work as well with those who choose to block the download in their browser.

7.4.8 Marketing Data

Worcester State must only collect consumer information that is pertinent and necessary for the purpose at hand. Worcester State must be sensitive to a consumer's expectation that some personal information may be considered confidential and should not be used for marketing. If the College contributes student or other client data to a cooperative database, the security of the database must be verified to be equivalent to or greater than that applied at Worcester State; and the organization's privacy policy must be reviewed before information is released.

7.4.9 Data accuracy

Worcester State must have the means to update its student/client data. All student/client data must be reviewed and/or revised on a regular basis. All student/client inquiries regarding data accuracy must be answered promptly and to the student/client's satisfaction.

7.4.10 Site Privacy Statement

Sample Site Privacy Statement:

- We do not collect personally-identifiable information on our web site or otherwise unless you choose to give it to us via an electronic mail message, SSL-protected Web communication, a phone call, or postal mail. Even when you choose to give us information, we keep it strictly confidential.
- We do not sell, rent, share, or otherwise disclose mailing lists or other personally identifiable information. We maintain some records of individuals who contact us in case we contact you later or provide further information to you in the future. However, we do not provide this information to anyone else unless you give us your permission in writing.
- We do not share names or other identifying information unless you specifically authorize us to do so in writing.
- We do not enable "cookies" on our Web site. The server of our Internet Service Provider (ISP) collects information about the date and time in which our Web site was accessed and the Internet address of the Web site from which you linked to our site. We have the ability to access this information, but we have chosen not to avail ourselves of this data for the time being. If we decide to use this information to analyze Web traffic in the future, we will only be able to measure the number of visitors to our site and the addresses of the Web sites from which our visitors come. E-mail addresses and other personally identifiable information are not available to us.
 - [NOTE: If a particular site uses cookies to provide session tracking for secure applications, this section should be revised accordingly to accurately reflect what information is stored in the cookie and why.]
- At Worcester State, we intend to give you as much control as possible over your personal information. In general, you can visit Worcester State sites without telling us who you are or revealing any information about yourself. There are times, however, when we may need information from you, such as your name and address.
- It is our intent to let you know before we collect personal information from you on the Internet.
- If you choose to give us personal information, via the Internet, that we or our business partners may need to correspond with you, process an order, or provide you with information, it is our intent to let you know how we will use such information. If you tell us that you do not wish to have this information used as a basis for further contact with you, we will respect your wishes.
- We do keep track of the domains from which people visit us. We analyze this data for trends and statistics, and then we discard it.

7.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For individual employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

8. Information Valuation and Protection Policy

8.1 Policy Statement

All Worcester State business information must have its value determined and be categorized to ensure that proper protection is afforded the information during its life cycle.

8.2 Applicability

This policy applies to all members of the Worcester State College community.

8.3 Justification

All Worcester State information and assets must be protected, including the information critical to its operation and continued viability as a business entity. The current business environment is highly dependent on the creation, exchange, and storage of information in electronic and magnetic form, using stand-alone computers, and computers that are interconnected over local- and wide-area networks.

Unlike traditional paper and paper-based files, information in electronic media can be extremely vulnerable to both inside and outside threats. Electronic information transfer is susceptible to unauthorized access, disclosure, manipulation, or compromise by a very unsophisticated threat element.

8.4 Minimum Implementation Standards

8.4.1 Information Valuation and Categorization Guidelines

To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the need and requirements for security protection.

Business information assets are those that affect and are integral to the following areas:

- Business growth
- Ability to comply with laws and regulations
- Integrity and public trust

All information assets must be valued and categorized for protection as either critical business or public information. Critical business information assets are defined as any information whose exposure to theft, loss, unauthorized alteration, or unavailability could affect competitiveness and business growth, the ability to comply with laws and regulations, public trust, or the integrity of Worcester State. Critical business information is data to which permitted access is normally limited and disclosure of which could damage or threaten the College's interests or competitiveness. Critical business information assets should be categorized using one of the following definitions based on the potential impact it has on the business if it were lost, stolen, destroyed, altered, or if its use were denied. All sensitive business data requires special marking and handling requirements.

The classifications are:

- **Worcester State Confidential Proprietary Information:** Information that is proprietary to Worcester State that may cause the College competitive harm if it is disclosed to individuals who are not under a duty of confidentiality to the College either by way of non-disclosure agreement, employment, or other fiduciary relationship. This information should be protected from inadvertent disclosure to non-employees and others who do not have a duty of confidentiality to the College. Additionally, access within the College may be restricted to certain employees on a need-to-know basis. Examples include product development, marketing, sales, and operations information.
- **Third Party Proprietary Information:** Information that is proprietary to a third party, e.g., a student, client, supplier, or former employer of a Worcester State employee that is protected by a non-disclosure agreement between the third-party and Worcester State or a Worcester State employee. This information should be protected to the degree required by such non-disclosure agreement.
- **Financial Information:** Information related to the financial performance of the College. This information should not be disclosed outside the College without the approval of the appropriate Vice President or the President, and access within the College should be provided to employees on a need-to-know basis only.
- **Employee Information:** Confidential information regarding employees that must be protected for privacy reasons. This information should not be disclosed outside the College without the approval of the head of Human Resources, General Counsel, or the President, and access within the College should be restricted to a limited number of employees and managers on a strict need-to-know basis.
- **Legal Information:** Confidential legal information should not be disclosed outside the College without the approval of the General Counsel or the President, and access within the College should be restricted to a limited number of employees and managers on a strict need-to-know basis.
- **Public Information:** Public information assets include, but are not limited to:
 - Non-private information for students/clients
 - Current advertisement information
 - Public financial disclosures
 - Press releases
 - Other information generally considered publicly available
- Business information assets may be categorized as Public only if the information or assets are being freely distributed internally and externally to Worcester State, are freely available outside of Worcester State or are intended for public use.
- Valuation of information should be assessed regularly:
 - Critical business information must be evaluated, valued, and categorized on, at least, an annual basis.
 - To ensure that appropriate protection is provided, the value of information should be determined before release or transmission over any communications network.

8.4.2 Storage

Storage requirements are determined based on the sensitivity of the information and the facility in which it is located. Care must be exercised to avoid unauthorized disclosure of Privacy Act data. Access to Privacy Act information should be limited to authorized users having a need for the information in the performance of official duties. Sensitive records such as medical, financial, and personnel records or criminal investigations should be kept in lockable metal file cabinets or in a secured room at all times.

8.4.3 Transmission

Transmission of Worcester State information includes the movement of project related information by mail, courier, delivery service, or electronic means (including, e-mail, facsimile transmission, file transfer protocol, etc.). Transmission of data through the Internet exposes the local computing environment to threats, such as hacker attacks, unauthorized data disclosure, and viruses. The Data Security Officer is responsible for ensuring that the computing environment is operating at an acceptable level of risk.

8.4.4 Information Protection

Protective measures must take into account the business impact (value) associated with unauthorized access or damage to critical business information assets. Worcester State must develop procedures for the secure handling of all critical business information assets. These procedures must be documented in the form of an Information Valuation and Categorization Guide and Safeguards document for each major business area or organization.

No protection against disclosure is required for Public information assets. The Data owner is responsible for determining the appropriate value and categorization of the information generated by the owner, or organization. While public information is not required to be protected during transmission or transfer, use of available protection mechanisms, especially for data integrity concerns, is encouraged. Public information may be exchanged over the Internet, but consideration should be given to the use of other, more secure methods when they exist.

8.4.5 Information Marking/Labeling

Information entering, leaving and within systems or processes must be marked appropriately. The formats that must be considered for labeling are:

- Printed paper reports, memoranda, spreadsheets, documents, and letters
- Screen displays
- Magnetic media (disk, tape, etc.)
- Electronic messages and file transfers
- Other similar information media

8.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

9. Computer and Network Security Policy

9.1 Policy Statement

Access to all Worcester State networking and computing resources must be based upon strong identification and authentication.

9.2 Applicability

This policy applies to all members of the Worcester State College community.

9.3 Justification

Worcester State networking and computing resources are vital assets that must be protected.

9.4 Minimum Implementation Standards

9.4.1 Access Management

Users must be positively identified and authenticated prior to being permitted access to any Worcester State network or computing resource. Remote access to Worcester State messaging systems from home or for mobile users, using personal or college-owned computers, over public networks (PSTN, Internet) is permitted. Remote users must use strong authentication in accessing computer or network resources. Users working in non-Worcester State facilities, using facility-provided workstations or networks, are not permitted access to Worcester State networked systems.

9.4.2 Account Management

Attempting to access another user's accounts is prohibited. This includes access through e-mail system client software or through capture of data traversing the network. Creation of all accounts must be performed only by authorized system administrators and only after receiving documented management approval for each new account.

Accounts will be deleted immediately upon termination or transfer of employment of the user. All messages will be permanently deleted from the user's mailbox (but may be archived elsewhere), and delivery of any further messages to the account will be prevented. Account retention or forwarding, after termination of employment, is not permitted without prior written management approval.

9.4.3 Information Transmission

Information transmitted or accessed over the Worcester State enterprise network must be protected commensurate with its value and handling category established by the information owner.

9.4.4 Monitoring

Worcester State reserves the right to monitor the content and traffic patterns and/or electronically screen networking and computing resources, including activity and traffic originating remotely. Purposes for such monitoring and/or screening include, but are not limited to, system maintenance, detection and elimination of contamination, detection and prevention of unauthorized disclosures of Worcester State confidential or proprietary information, detection of unauthorized access to computing and network resources, and determination of compliance with Worcester State policies.

Worcester State reserves the right to intercept and/or quarantine any networking or computing resources that may pose a threat to Worcester State, including, but not limited to, data, messages, and network traffic. If such monitoring, screening, interception, and/or quarantine reveal possible evidence of criminal activity, Worcester State may provide the evidence of such monitoring to law enforcement officials.

9.4.5 Reporting of Suspected Violations

Users must report any suspected violation of these policies to the Data Security Officer. All reports of alleged violations of this policy will be investigated on a case-by-case basis. During the course of the investigation, access privileges will be monitored and may be suspended. Violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or termination of employment.

9.5 Moves, Adds, and Changes

Administrators must maintain tables, diagrams, and other records of baseline system and security configuration, and any configuration changes for all user hardware and software system components. Inventories must be kept of all the hardware with type, model, purpose, and location. A software inventory with version, patch level, installation options, purpose, location, license numbers, and keys must be kept and provided to the Data Security Officer. Any time there is a relocation of personnel, equipment, or software the inventory list must be updated and a copy provided to the Data Security Officer.

9.6 Escalation

In accordance with the Incident Reporting and Response Policy, security incidents must be reported to the next higher entity on the security point of contact list created by the Data Security Officer. The point of contact list should include information about how to contact them: (home phone number, office phone number, cell phone number, home and office email address, and pager numbers).

9.7 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For individual employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

10. Internet and WWW Security Policy

10.1 Policy Statement

Access to the Internet and World Wide Web (WWW) using Worcester State network or computing resources must be implemented in a secure manner to protect critical business assets and information.

10.2 Applicability

This policy applies to all members of the Worcester State College community.

10.3 Justification

Internet and WWW services access is provided as a business tool and an information conduit to assist in the accomplishment of the College's educational and business goals.

10.4 Minimum Implementation Standards

10.4.1 Access Control

Access to the Internet from Worcester State network resources requires prior management approval. Users must authenticate their identities before being permitted access to the Internet. Worcester State reserves the right to filter content and monitor sites that may be accessed via any Enterprise Internet connections.

10.4.2 Protection of Network and Computing Resources

The Internet or WWW must never be used to communicate Worcester State proprietary or confidential information, unless the confidentiality and integrity of the information is assured and the identity of the recipient(s) is authenticated. All policies governing remote access and the use of messaging resources must be adhered to when using the Internet for remote access to Worcester State.

Users are required to comply with local and international laws governing the use of protection software when selecting appropriate safeguards for Internet use. The Data Security Officer must approve all protection mechanisms used. Users must ensure that precautions are taken to protect Worcester State's networking and computing resources when obtaining software, files, and data from the Internet.

Users have the responsibility of ensuring that all software, files, and data entering Worcester State's computing environment are properly scanned for all potential contaminants, including, but not limited to, viruses, malicious programs, malicious applets, and "Trojan Horse" functionality. Users must not intentionally develop, download, or otherwise install programs or other software that will infiltrate a network or computer resource and damage or alter the software, hardware, or information contained on the network or computer resource.

10.4.3 Web Browsing and General Internet Access

Access from Worcester State enterprise networks and/or systems to the Internet requires management approval and must never be used to communicate Worcester State confidential, proprietary, or other sensitive college information unless properly protected with a Worcester State approved mechanism. Worcester State employees are not allowed to use the Internet for recreational games or for obtaining or distributing pornographic, sexually explicit, or non business-related materials.

Employee use of the Internet may be monitored for inappropriate use and impact to productivity. Users are required to respect and comply with local and international legal protection provided by trade secrets, patents, copyrights, and trademarks to any information viewed or obtained via the Internet. No copyrighted software may be downloaded for the purpose of use and/or further distribution to Worcester State's networking and computing resources without the proper license to use and/or distribute such software.

10.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

11. Password and PIN Security Policy

11.1 Policy Statement

Passwords and PINs must be properly structured, routinely changed, and kept strictly confidential.

11.2 Applicability

This policy applies to all members of the Worcester State College community.

11.3 Justification

The User ID, or account identifier, today is the foundation of information security. It is used to grant privileges and access rights to users and then to account for their actions. At present passwords and PINs are used to authenticate the owner of the User ID. Secure use of passwords and PINs for user authentication requires effective password or PIN construction, observation of password/PIN life expiration, and maintenance of password or PIN confidentiality.

11.4 Minimum Implementation Standards

11.4.1 Password/PIN Confidentiality

All passwords and PINs must be handled as Worcester State Confidential, and the individual user must keep passwords and PINs for all accounts secret. At no time are user IDs, passwords, or PINs to be shared with others. System designs should not permit passwords to be displayed on the screen as they are entered. All passwords and PINs must be changed whenever there is any indication of possible system or password compromise.

Passwords and PINs must always be encrypted when held in storage for any significant period of time or when transmitted across the network. One-time passwords are the exception. Passwords and PINs must never be embedded in sign-on utilities. For example, users must never be able to authenticate at sign-on merely by using a function key or by running an available program.

11.4.2 Password/PIN Length

Passwords and PINs must have a minimum length of eight (8) characters. Passwords and PINs for privileged accounts and accounts requiring strong authentication must have a minimum length of ten (10) characters. Privileged accounts are those with administrator privileges (for example, the ability to modify system parameters, audit users' activities, or bypass normal security measures) or with privileges that exceed those provided to typical users.

11.4.3 Password Complexity

Passwords must contain characters using English upper case letters, English lower case letters, Westernized Arabic Numerals, and non-alphanumeric symbols, and consist of at least three from these four classes. Passwords must not be derived from commonly used words or phrases or easily guessed words found in English or non-English dictionaries, nor may any given character appear more than twice.

11.4.4 Password/PIN Expiration

Passwords and PINs for general users accounts must be changed at least every ninety (90) days. Privileged accounts must be changed at least every thirty (30) days. Temporary and initial passwords and PINs must be marked as expired, and users must be required to change the password/PIN at the first use.

11.4.5 Default Passwords/PINs

Any default password or PIN for a given operating system or software package must be changed immediately upon the completion of the installation process. The new password or PIN must conform to the requirements defined within this standard. Default accounts must be renamed, if possible, to non-obvious names.

11.4.6 Password/PIN Reuse

User-chosen passwords and PINs must not be reused for five (5) iterations. Temporary passwords or PINs issued by a help desk or administrator must be changed on a daily basis and must not be reused for at least six (6) months. Users may only implement a password change once per day.

11.4.7 Password/PIN Changes

Proper proof of identification must be provided before changing a password or PIN. Users changing a password or PIN via a system command or screen must prove knowledge of the current password or PIN before being allowed to change it. Users requesting a new password or PIN, or requesting a password or PIN change/reset, must prove their identities before the change is initiated.

The new or reset password or PIN must be delivered in accordance with the requirements documented below in Password/ PIN Delivery. The new or reset password must be treated as a temporary password, as documented above in Password/PIN Expiration. The new or reset password must conform to the Password Length and Password Complexity requirements documented above. If a transferred, resigning, or terminated staff member was responsible for system administration, all relevant passwords must be changed immediately.

11.4.8 Password/PIN Delivery

Delivery of passwords to a user, either when an account is created or when an administrator resets a password, requires attention to ensure that delivery is done efficiently and securely. Passwords must not be transmitted over any Worcester State voice, video, or data network without appropriate identification and authentication. A clear-text User ID and associated password must never be delivered in a single message or via the same medium (e.g., both delivered to the same voice mail box).

A password must be delivered in a manner that requires the recipient to prove his/her identity before the password is received. A User ID and associated password may be delivered in a single message via a single medium if, and only if, the confidentiality of the message is protected using strong encryption that provides for both confidentiality of the message content and authentication of both the sender and recipient.

11.4.9 Emergency Delivery of a One-Time Password

A one-time password or token card code (**not** a temporary password) may be provided via a telephone call to a user who has lost or forgotten his/her token card, so long as the user has authenticated himself, as documented above in Password/PIN Changes.

11.4.10 Policy Enforcement

Administrators are accountable for configuring systems to enforce this policy. Where possible, the system must enforce these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures. For example, to enforce password complexity, the administrator can run tools to crack passwords, at least monthly, and require users with weak passwords to change their passwords.

11.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

12. Account Management Security Policy

12.1 Policy Statement

All Worcester State user accounts must be managed to assure strict control of account establishment, use, and timely removal when appropriate.

12.2 Applicability

This policy applies to all members of the Worcester State College community.

12.3 Justification

The User ID or account identifier is the foundation of information security. It is used to grant privileges and access rights to users and then to account for their actions. The effective management of accounts is critical to maintaining a secure environment.

12.4 Minimum Implementation Standards

12.4.1 New Accounts

New accounts must be created with the minimal set of privileges necessary. The Data Security Officer must grant additional access rights and privileges. The manager responsible for the resource must approve the granting of administrator access rights and/or privileges, or the creation of an account with any administrator access rights and/or privileges. Accounts with administrator access rights and/or privileges must be reviewed by management semi-annually and re-authorized annually.

12.4.2 Unused Accounts

User account(s) must be deleted immediately upon an individual's transfer or termination of employment. All new accounts that remain unused for seven (7) days must be disabled. Any accounts that remain unused for forty-five (45) days must be disabled, and any accounts that remain unused for ninety (90) days must be deleted.

12.4.3 Failed Login Attempts

Accounts must be disabled after three (3) attempts to login with an invalid password.

12.4.4 Policy Enforcement

Administrators are accountable for configuring systems to enforce this policy. Where possible, the system must automatically enforce these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures.

12.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

13. Remote Access Security Policy

13.1 Policy Statement

Remote access to Worcester State networks and computing resources requires strong identification and authentication.

13.2 Applicability

This policy applies to all members of the Worcester State College community.

13.3 Justification

Remote access services, if implemented, allow access to network and computing services for users who are not directly connected to the Worcester State enterprise network. Dial-in connections, ISDN, or virtual private network technology can provide remote access over the Internet.

13.4 Minimum Implementation Standards

13.4.1 Centralized Access

Any dial-in access to Worcester State's resources must be limited to authorized entry points. The telephone numbers used for dial-in must not use the same exchange as Worcester State's published numbers. Modems on desktops, laptops, and servers are not authorized entry points.

Authorization requires a security assessment of the architecture, design, practices and operations of a remote access service, as well as periodic re-assessment. All inbound connections to the Worcester State enterprise network and/or multi-user computer systems connected to the Worcester State enterprise network must pass through an access control system such as a firewall, modem pool, telecommunications front-end, or similar system prior to being permitted to reach a log-in prompt.

13.4.2 Authentication

Users remotely accessing the Worcester State network must be authenticated using strong authentication mechanisms. Strong authentication mechanisms include one-time pass codes, token cards, or cryptographic-based authentication. Upon management approval, a User ID and reusable password may be used provided they are transmitted over an encrypted session.

Users are responsible for maintaining the confidentiality of IDs, passwords, token cards, and corresponding PIN codes that are given or assigned in conjunction with the remote access service. A User's passwords and PIN code should never be written down and never carried with the token card. Token cards and passwords must never be shared. Users are responsible for the physical security of their token cards or smart cards. Users are accountable for any harm resulting from disclosure of any password/access codes or the loss of any token or smart card. Any breach or potential breach, disclosure of a password or PIN code, or loss of a token card must be immediately communicated to the Data Security Officer.

13.4.3 Management Authorization

Management approval is required before a user is authorized to use remote access services. Remote access permissions must be reviewed and re-authorized annually by the user's management.

13.4.4 Protection of Worcester State Information and Computing Resources

Users must protect the confidentiality and integrity of any data that is accessed remotely. This includes, but is not limited to, ensuring that any Worcester State data is either erased from the remote device or protected appropriately, based on the sensitivity of the information. Remote device is defined as a laptop or desktop computer, palmtop device, or personal digital assistant device used to access remote access services.

Users must ensure that the remote access service provides sufficient privacy for the sensitivity of the data being accessed. If uncertain, Users should seek the guidance of the information security staff before remotely accessing highly sensitive information. Users must ensure that precautions are taken to protect Worcester State networking and computing resources when uploading software, files, and data from the remote device to the Worcester State enterprise network. Users have the responsibility of ensuring that all software, files, and data entering Worcester State's computing environment are properly scanned for all potential contaminants including, but not limited to, viruses, malicious programs, malicious applets, and "Trojan Horse" functionality.

Only Worcester State approved remote devices may be used to access remote access services. Any device used to access remote access services must conform to all Worcester State policies including, but not limited to, Worcester State policies noted above. The use of personal or non-Worcester State issued remote devices requires the approval of local Worcester State management and an agreement with the User that the device will be maintained in accordance with all Worcester State policies.

All Worcester State owned remote access software and hardware must be returned upon a User's end of employment or elimination of the need for remote access. Remote access via the Internet must be protected with strong encryption. The use of strong encryption must be enforced at the point of entry to the Worcester State enterprise network. Strong encryption is defined to be at least a 128-bit key for symmetric encryption.

13.4.5 Remote Access by Non-Worcester State Employees

Users who are not Worcester State employees must coordinate with the Data Security Officer for access.

13.4.6 Session Management and Audit

Users should disconnect from the remote access connection when not actively using it. Users must be disconnected after sixty (60) minutes of idle time. Users must not use any automatic method to avoid the inactivity disconnect. Remote access sessions to critical business information assets must be audited. For each remote session, the time, date, duration, and User ID must be recorded. Worcester State reserves the right to monitor the content and traffic patterns and/or electronically screen networking and computing resources, including activity and traffic originating remotely. Computer usage by these users will be audited for appropriate use and productivity.

13.4.7 Diagnostic Access

Dial-up access for diagnostic purposes from vendors or system administration personnel that provides direct access (i.e., bypasses required access control points) must be provided only as needed and used only when the enterprise remote access service is unavailable or does not meet the requirements for diagnostic access. Such access may be enabled only for the duration of the required diagnostic or maintenance activity and must be disabled immediately upon its completion by physically unplugging cables and/or turning off equipment.

13.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

14. Vendor/Consultant Access Security Policy

14.1 Policy Statement

Vendor or consultant access to Worcester State network or computing resources is permitted only when restricted and tightly controlled.

14.2 Applicability

This policy applies to all members of the Worcester State College community.

14.3 Justification

Vendors or consultants with whom Worcester State has a close association may require access to Worcester State network and computing resources such as remote access, e-mail, and file and print services. With proper business justification, an account to a specific individual from a Vendor/Consultant company can be approved when requested by a Worcester State employee (the Sponsor) and approved by the Sponsor's manager.

The Vendor/Consultant Company is ultimately responsible for this account and bears responsibility for the conduct of its employees; however, the sponsor is responsible for ensuring that the Vendor/Consultant users are aware of, and adhere to, all Worcester State policies, including the Personnel Security Policy. Each Vendor/Consultant user must have in effect an individual, Non-Disclosure Agreement with Worcester State or the subordinate organization. The Sponsor must submit a completed Request for Vendor/Consultant Access form. The Sponsor must specify the reason and need for access to Worcester State network and computing resources, keeping in mind the confidential nature of the accessible information.

Once the request is received, the account will be created. The data owners will determine all Vendors/Consultants access.

14.4 Minimum Implementation Standards

14.4.1 Security Policy Compliance

Access to Worcester State network and computing resources is granted solely for the work contracted and for no other purposes whatsoever. Access to any additional resources requires express, written consent from the information owner as supported by the Sponsor and the Sponsor's manager.

No account may be shared. If there are multiple personnel from a vending/consulting company, a separate account is required for each Vendor/Consultant employee. Vendor/Consultant Company's access to Worcester State network and computing resources may be terminated immediately upon Worcester State learning of any violation of the terms of this agreement or misuse of the system. Misuse includes, but is not limited to:

- Sharing a password or an account with any other person
- Introducing any foreign files onto the system
- Attempting to access Worcester State information/applications, other than those authorized
- Failure to comply with this agreement
- Violation of Worcester State security or acceptable use policies

Vendor/Consultant companies will immediately notify the Sponsor when a Vendor/Consultant user with access to Worcester State network and computing resources no longer needs access. This could result from a change in assignment or employment status.

14.4.2 Sponsor Responsibilities

The Sponsor must, if requested, provide a printed copy of the Worcester State policies listed above. The Sponsor must immediately report any suspected violation of this agreement to his/her management and to the local remote access administrator. The Sponsor is accountable for the activities of the Vendor/Consultant user. The Sponsor is responsible for initiating necessary action to delete the account when it is no longer required. The Sponsor is responsible for semiannually reviewing the need for the Vendor/Consultant account.

14.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

15. Access Control Gateway Security Policy

15.1 Policy Statement

All network interconnections between any external network and the Worcester State enterprise network must be protected by an access control gateway.

15.2 Applicability

This policy applies to all members of the Worcester State College community.

15.3 Justification

The growing need to connect the Worcester State enterprise network to external networks, including the Internet, as well as business partner networks, presents a critical necessity to ensure that the integrity and security of the Worcester State enterprise network is not compromised by these connections.

15.4 Minimum Implementation Standards

15.4.1 General

All external accesses to the Worcester State enterprise network must pass through an access control system (such as a firewall), where all traffic between the enterprise network and external networks can be controlled, monitored, and examined for any access violations.

15.4.2 Periodic Assessment

Authorization requires a security assessment of the architecture, design, practices and operations, as well as periodic re-assessment. There must be the capability to demonstrate and periodically validate that the claimed level of security protection is being enforced, and confirmation that the system carries out policy rules.

15.4.3 Access Control

The enterprise network must be protected by at least one authorized firewall that defines and enforces rules over information and users crossing internally to external systems, or from external systems to internal resources, including Worcester State information services provided via a Service Segment (e.g. a Demilitarized Zone [DMZ]).

Firewalls must employ a strong authentication process to verify a user's identity (login and related password) before access to the Worcester State's internal network is granted. Strong authentication mechanisms include a one-time password, token cards, or a cryptographic-based method of authentication. With management approval, a User ID and reusable password may be used if transmitted over an encrypted session.

All access to the Worcester State enterprise network must have an approved business purpose and associated risk assessment. Remote users may not access Worcester State systems through unauthorized modems placed behind a Worcester State firewall.

All Worcester State firewall servers must have inbound and outbound rules to specifically allow or deny connections. All access not explicitly allowed must be denied. All traffic to/from the enterprise network must employ application-level proxies, whenever possible. If no application proxy exists, it is the responsibility of the Data Security Officer to determine if the traffic will be allowed, using packet-filtering or stateful inspection processes.

15.4.4 Configuration

All Worcester State owned and operated firewall servers must be equipped with approved, dynamic intrusion detection and alerting mechanisms. Intrusion thresholds must be set so that automated alarms and/or preventative actions are initiated. All Worcester State firewall server configurations will be reviewed quarterly. Firewall rules to prevent source routing and spoofing attacks must be included in the configuration. All changes to the firewall require a risk assessment and must be approved prior to implementation.

If a Worcester State firewall requires an operating system, a secured version of the operating system, with all patches installed, must be a part of the firewall. These patches must be installed not later than forty-eight (48) hours after their availability from the vendor. (Note that there should be an identified need for the patch in the Worcester State computing environment and that the patch should first be tested offline to ensure it will not cause instability or malfunction before being introduced into production systems.) Firewall passwords must follow the standard Worcester State policy for equipment of this type.

15.4.5 Logging and Auditing

All Worcester State firewall servers must contain mechanisms for logging traffic, suspicious activity, and must contain mechanisms for log reduction to ensure that logs are readable and understandable.

15.4.6 Administration

Firewall passwords must be recorded and securely maintained. Knowledge of firewall passwords and rules must be restricted to the minimum number of people necessary. Worcester State firewall server consoles must not display the last user to log in. All Worcester State firewall servers must be logged off when unattended.

All Worcester State computers or network control devices (e.g., router, switch, and hub) must display the following legal notice/warning message to deter theft of data and equipment.

“WARNING NOTICE This system is restricted solely to Worcester State users for legitimate business only. The actual, or attempted, unauthorized access, use, or modification of this system is strictly prohibited by Worcester State. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. If such monitoring and/or recording reveals possible evidence of criminal activity Worcester State may provide the evidence of such monitoring to law enforcement officials.”

This message must precede the login process, when possible.

15.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

16. Portable Computer Device Security Policy

16.1 Policy Statement

All portable computing devices used to process and store business information must be controlled, physically protected, and must employ appropriate security for its contents.

16.2 Applicability

This policy applies to all members of the Worcester State College community.

16.3 Justification

Laptops are a popular option for enterprise computer users with a need to work while away from the office. Handheld PCs, Palm-size PCs, and Portable Digital Assistants are proliferating as productivity enhancements. However, their portability, value, and the value of the information that is often stored on these portable-computing devices, makes them a target for theft. Employees are responsible for the portable-computing devices under their control, and must take the appropriate steps to protect the device and the information it contains.

16.4 Minimum Implementation Standards

16.4.1 Protection of Access

Where available, a power-on, BIOS, or security password must be enabled and a strong password used. Automatic login scripts, which would allow an unauthorized party to get into an account without requiring a password, are prohibited. Any authentication tokens (SecurID cards, smart cards) must be kept separate from the portable computing device and its case. Portable computing devices must not be left unattended when remotely connected to the Worcester State enterprise network, even if physically secured.

16.4.2 Protection of Data

Proprietary or confidential information must be protected, especially when outside of Worcester State controlled facilities. Up-to-date anti-virus software (including virus definitions) must be installed and automatic scanning enabled. All foreign media or files should be scanned before any files are opened.

Backup of any data stored on the portable computing device is the responsibility of the employee. Users are recommended to back up important files to the network drive when in the office or to removable media if a network drive isn't available. Proprietary or confidential information must not be accessed in public places (such as on an airplane) unless the employee is certain that only he can read the information on the display.

It must be emphasized that the significance of the loss of these types of computers lies in the information stored on them, thus it is important to maintain the physical security of these devices as well. Hard disk drives contain large quantities of information that can be accessed easily if the computer is lost or stolen. This information may be business-critical in nature and must, therefore, be afforded special protection. Laptop computers, which contain stored, business-critical information, must be afforded the same level of protection as the information that they contain. The use of authorized encryption software to encrypt the hard drive and protect it from access is strongly encouraged.

16.4.3 Equipment Identification

The employee should carry the brand, model number, and serial number separately from the portable computing device and case so that accurate information is available in the event of a loss.

16.4.4 Report Losses

Loss of a portable computing device must be reported to the Data Security Officer, Enterprise Security Investigation, and to the Data owner within twenty-four (24) hours of the loss. When good judgment has not been exercised in safeguarding a portable computing device, the employee may be held responsible for the replacement cost if the device is lost or stolen.

16.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

17. Encryption Policy

17.1 Policy Statement

Encryption used to protect critical business information must be in accordance with Worcester State cryptographic standards and practices.

17.2 Applicability

This policy applies to all members of the Worcester State College community.

17.3 Justification

Encryption greatly increases the level of effort and difficulty for unauthorized users to gain access to sensitive or confidential data, and reduces the potential for accidental disclosures.

17.4 Minimum Implementation Standards

17.4.1 Employment

Enterprise information may not be encrypted by anything other than Worcester State approved encryption algorithms and supporting processes.

17.4.2 Encryption Process

Users must verify that encrypted information can be decrypted before deleting the original, clear text data. Data recovery encryption key escrow must be performed in accordance with processes approved by the Data Security Officer.

17.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

18. System and Application Development Security Policy

18.1 Policy Statement

All systems and applications to be deployed on any Worcester State server or network must address security requirements during all phases of the development cycle.

18.2 Applicability

This policy applies to all members of the Worcester State College community.

18.3 Justification

Information security functionality must be fully integrated into the design of a new system, from the beginning, for it to be effective. Too often, security considerations are an afterthought that adds complication and cost to the development process. An up-front commitment to security will help ensure overall success of the end product.

18.4 Minimum Implementation Standards

18.4.1 Security Requirements Analysis and Specifications

The information owner and valuation of the information stored, processed, and communicated by the system must be determined prior to the development of security requirements and specifications. A comprehensive security requirement analysis and specification must be performed for all new systems and applications or significant upgrades to existing systems. System security requirements and specifications must be compatible with enterprise standards for technologies and system configuration, where applicable. System security requirements and specifications must require interoperability with all information sources and services with which it must interface. System security requirements and specifications must ensure integration with the existing security services, where applicable. Additional security assessment must be required to address any changes to the system functional baseline.

18.4.2 Security Verification and Validation

All new systems must be tested for stability and to identify any unanticipated side effects before they are introduced into the production environment. All new systems must be tested for security, integrity, and functional verification, in accordance with requirements and specifications, prior to general availability. Final approval of system security must be made at the CIO level within the College.

18.4.3 Custom Developed Software and Testing

Administrators must maintain records of any configuration changes for all software (messaging, database, Web, tape backup, security, etc.) and how and where they are installed. The data owner and valuation of the information stored, processed, and communicated by the system must be determined prior to the development of security requirements and specifications. A comprehensive security requirement analysis and specification must be performed for all new systems and applications or significant upgrades to existing systems.

Operational systems will not be used for development or testing activities. All security features and functions will be operated during formal acceptance and operational tests. Prior to bringing a new system or upgrade to an existing system on line, testing will be done to ensure the new system does not adversely affect the existing systems. New or major upgrades to an existing system will be certified for operation at the CIO level prior to operating the system in the production environment.

18.4.4 Unauthorized Installed Software

Administrators are accountable for unauthorized software that is used on machines under their control. Users are prohibited from installing executable or any unauthorized software on Worcester State computers. If automatic scanning of files is not enabled or anti-virus software is not installed on a server, the users and administrators must manually scan any floppies, compact discs, downloaded executables, or downloaded compressed files (i.e., zip files) on another system prior to deployment.

18.4.5 Commercial Off-the-Shelf Software

Administrators are required to maintain a software inventory with version, patch level, installation options, purpose, location, license numbers, and keys.

18.4.6 Copyright Law

No copyrighted software may be downloaded for the purpose of use and/or further distribution to Worcester State networking and computing resources without the proper license to use and/or distribute such software. Users are responsible for obtaining the license and permission from the holder of the copyrights to use and/or distribute copyrighted software.

18.4.7 Continuity of Service

A fallback plan must be devised for recovery of existing services in the event that introduction of a new system causes service degradation or interruption. A cutover plan must be written prior to rollout of a new system to ensure continuity of service.

18.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

19. Incident Reporting and Response Policy

19.1 Policy Statement

All suspected and confirmed security incidents must be reported.

19.2 Applicability

This policy applies to all members of the Worcester State College community.

19.3 Justification

An increasing amount of dependency is being placed on the enterprise network. At some point, there will be a disruption in the operation of the network. This disruption may be due to an attack from an intruder, equipment failure, act of nature, disgruntled employee, or user error. An incident is defined as any irregular or potentially adverse event that occurs on any part of the Worcester State enterprise network. Some examples are listed below:

- Compromise of system or data integrity (e.g., data has been accessed or changed without explanation)
- Denial of service (e.g., cannot access e-mail)
- Illegal access to a system or data (e.g., intrusion or penetration)
- Malicious use of any system resources (e.g., viruses)
- Any damage to a enterprise network asset (e.g., fire or water damage, power failure)

When these disruptions or incidents occur, they must be handled in the most expedient way both to restore network operation and to determine the cause of the fault in order to keep it from reoccurring.

19.4 Minimum Implementation Standards

19.4.1 Incident Reporting and Escalation

Local Data Security Officers or Data Security Administrators are responsible for monitoring the behavior of the systems or servers under their control. They must:

- Note any unexpected loss or changes in electronic data
- Note any suspicious behavior, such as requests for access or password information, by unauthorized persons
- Note any unauthorized network or host intrusion attempts.
- Report all incidents to appropriate authority.

Security incidents must be escalated up the management chain in a timely basis.

19.4.2 Internal Incident Response Team

The Internal Incident Response Team should be composed of the CIO, Data Owners, Data Security Officers, General Counsel, Enterprise Security and Investigation, a representative from Public Affairs, and system and network administrators for systems and technologies involved in the incident

19.4.3 External Incident Response Team

If the security or technical expertise required to resolve the incident and restore operations in a timely manner is not available on the Internal Incident Response Team, the Data Security Officer should identify an External Incident Response Team that can provide support as needed. The external team should be experienced with coordinating incident response on an international and Internet level, understand Worcester State operations and technology, and covered by a nondisclosure agreement. In addition to providing technical and security expertise, the external team can also act as a trusted agent in the event a security authority or administrator is suspected of being involved in an incident.

19.4.4 Incident Response Process

After a security authority declares the severity of the incident, and declare it an IT security incident, the Internal Incident Response Team should be immediately notified and called to a meeting to evaluate the information that is available and discuss options for resolving the problem. The Data Security Officer will be responsible for notifying and assembling an internal team in a timeframe proportional to the severity of the incident. The team should meet in person or by teleconference and gather to discuss information about the incident and determine the next course of action. If the decision is made to contact an external incident response team for help with an incident, only the CIO or Enterprise Security Officer is authorized to contact and initiate support from the external team.

19.4.5 Computer Investigations and Evidence

While the same legal principles apply to searches and seizures of computerized records as to other records, when the search is of records on a computer used for business the need for particularity is heightened since the material to be searched may be protected by the Fourth Amendment.

Should any government inquiry arise through the issuance of a written subpoena or written request for information, such request should immediately, and before any action is taken or promised, be submitted to the Office of General Counsel.

19.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

20. Intrusion Detection Policy

20.1 Policy Statement

Intrusion detection must be employed on all servers and networks that process or store critical business information.

20.2 Applicability

This policy applies to all members of the Worcester State College community.

20.3 Justification

Awareness of circumstances that may represent a security breach is an important part of ongoing security administration. It is imperative that problems be discovered at the earliest possible time to minimize damage or loss. That is the purpose of intrusion detection. Intrusion detection is a key element in any multi-layered security architecture. Authentication and access control are the first lines of defense; but, even if circumvented, intrusion detection can help identify and prevent further penetration.

20.4 Minimum Implementation Standards

20.4.1 Intrusion Detection Technology

Intrusion detection technologies that recognize both network and host attack signatures must be employed. Intrusion detection tools must be in accordance with Worcester State standards. Intrusion detection systems must use a centralized model for data collection and analysis.

20.4.2 Deployment

Intrusion detection sensors/agents must be installed on any local area network segment or host system on which critical computing or information resources reside. Critical resources include, but are not limited to: database servers, authentication domain servers, security servers, messaging servers, Web (http) servers, and file servers.

20.4.3 Configuration

The intrusion detection system must not be disabled to avoid excessive false alarms. Intrusion detection must be set to a sensitivity level that minimizes false alarms, while ensuring that critical events are not missed. Response options to suspicious activity or attack must include logging, paging, e-mail notification, running a user-defined process and session termination. Session termination must not cause denial-of-service from false alarms. Automated synchronization to a centralized time standard must be configured for all sensor/agent, data collection, and data analysis hosts to enable accurate correlation of logged events.

20.4.4 Data Management

Event logs must be monitored daily. Critical events must generate an alarm and be analyzed and responded to immediately. Log data may be required to establish a pattern of attack or abuse over a sustained time period, or to pursue legal action against a suspected intruder. Consequently, event logs must be archived for not less than ninety (90) days.

20.4.5 Incident Response

Security events must be reported in accordance with the Security Incident Reporting and Response policy. Significant security events must be documented, in writing, for dissemination to other enterprise security personnel within forty-eight (48) hours of first occurrence. Dissemination must be at the discretion of, and through, the Information Security Director.

20.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

21. Information System Asset Control Policy

21.1 Policy Statement

Worcester State owned information system assets must be documented and accounted for and their use must be controlled.

21.2 Applicability

This policy applies to all members of the Worcester State College community.

21.3 Justification

Asset tracking provides the ability to control resources, and prevent and detect losses.

21.4 Minimum Implementation Standards

21.4.1 General

This policy applies to all assets, both hardware and software, used to create, transfer, or store information for use by or for Worcester State.

21.4.2 Employment

Worcester State information management assets must have description of what is the asset, brand, make, model, and data owner recorded in a database for use in tracking and control. The owner of the asset must control all original documentation for Worcester State assets. Personally owned computers used to process, store, or transfer Worcester State information must be subject to the same enforcement as enterprise owned assets. Data on magnetic media must be erased/destroyed using a Worcester State approved method before discarding.

21.4.3 Loss of Enterprise Assets

Any loss of or damage to an enterprise asset must be reported to the data owner and Data Security Officer within twenty-four (24) hours of the loss. When good judgment has not been exercised in safeguarding an asset, the individual may be held responsible for the replacement cost if the asset is lost or stolen.

21.4.4 Enforcement

Asset information, as listed above, must be verified on a quarterly basis. Random asset inspections must be made to verify location and condition of assets. A database must be maintained to track all enterprise assets.

21.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

22. Configuration Management Policy

22.1 Policy Statement

Configuration management must be employed on all computing and communications software assets.

22.2 Applicability

This policy applies to all members of the Worcester State College community.

22.3 Justification

The failure to upgrade systems, install patches in a consistent and timely manner, and configure systems to eliminate known security weaknesses can create significant risk for the enterprise IT environment.

22.4 Minimum Implementation Standards

22.4.1 General

This policy applies to all Worcester State enterprise computing and networking assets.

22.4.2 Documentation

Worcester State must document the configuration of each computing and networking asset. The documentation must contain a unique identifier, operating system (OS), versions, patches, and dates of patch. A listing of all software titles installed on each platform, with version, batches, and dates the patches installed are to be included in the documentation.

22.4.3 Software Updates and Patches

Software updates and patches must be researched, tested, and verified by appropriate personnel before installing on any Worcester State asset, and only applicable upgrades and patches can be applied to enterprise assets. Updates for common software titles used by Worcester State must be made accessible to all users of the Worcester State enterprise network after testing has been completed. Software updates and patches must only be acquired from the approved Worcester State enterprise network location. A list of approved software packages and version numbers for use on computers connected to the Worcester State enterprise network must be posted and made assessable to all users of the network. Critical security patches must be applied within 48 hours of their availability.

22.4.4 Standard Software Configurations

Standard configurations must be documented for, but not limited to, the type of OS. Configurations must include any modification that is not made by the “out of the box” default install (e.g., IP address of a server). Configurations must include any security-related modifications, and must be approved by the Data Security Officer who will inform the CIO. Configuration documentation must be made assessable to all users of the Worcester State enterprise network.

22.4.5 Software Other Than Standard

If other-than-standard software is required to perform an employee’s duties, authorization from his/her manager is required. The CIO to ensure that it is compatible with the Worcester State enterprise network and all associated Policies must evaluate any other-than-standard software.

22.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

23. Government Regulation Compliance Policy

23.1 Policy Statement

All Worcester State information and information system protection solutions must comply with all applicable government laws, regulations, and directives.

23.2 Applicability

This policy applies to all members of the Worcester State College community.

23.3 Justification

Government regulation affects a wide range of core Worcester State business activities. The primary purpose of regulation is to protect consumers, however, it also benefits industry by providing consistent standards and practices to which all must adhere. It is incumbent on all staff to ensure regulatory compliance, and information systems security plays a prominent role in that process. Failure to comply could expose the College to a range of serious consequences including litigation, loss of revenue, loss of market share, and loss of public trust and confidence.

23.4 Minimum Implementation Standards

23.4.1 Protection Solution(s)

Worcester State must evaluate its information system assets relative to government regulation and compliance to ascertain what data and resources require protection, their criticality, and the appropriate protection mechanisms.

Protection solutions must directly address:

- Confidentiality, integrity, authenticity, and availability of information assets.
- Control and accountability for system and information asset access.

Analysis, design, and implementation of security and protection services must be performed in accordance with Worcester State Information Asset Policies.

23.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.

24. Continuity of Operations and Disaster Recovery

24.1 Policy Statement

Worcester State must institute and practice an information systems disaster recovery plan that will prevent catastrophic data loss and ensure timely restoration of network and computing services in the event of system failure or destruction.

24.2 Applicability

This policy applies to all members of the Worcester State College community.

24.3 Justification

Business operations continuity is essential to protect competitive position, preserve public confidence, and protect against litigation.

24.4 Minimum Implementation Standards

24.4.1 General

This policy presents guidance on minimum content for a disaster recovery plan and is not the plan itself. Furthermore, it is not meant to be comprehensive and all encompassing in the area of business continuity management. It focuses on the information systems aspects of disaster recovery and does not cover the related areas of contingency planning, crisis management, and emergency management. Therefore, expansion of this policy, as appropriate, is permitted and encouraged.

24.4.2 Prioritization

Determine criticality of systems and impact of loss. Should be system and application-specific.

24.4.3 Prevention

The CIO and the Data Security Officer are to identify mechanisms that maximize availability and prevent information loss, such as fault-tolerant hardware, automatic fail-over hardware, non-interruptible power supply, and fire protection and prevention systems.

24.4.4 Roles and Responsibilities

The Data Security Officer must designate responsible individuals to perform specific duties related to plan development, plan maintenance, plan testing, and disaster recovery. The duties must be clearly defined, documented, and should include authority levels. These duties must be reviewed and or revised annually.

24.4.5 Documentation

One of the most crucial resources for reconstructing a failed system is complete, accurate, and up-to-date documentation. It is imperative that all information related to system design, configuration, and administration be continuously maintained.

24.4.6 Data Backup

System Administration Security Policy should contain a complete description of data backup requirements. This policy should stipulate all requirements and processes for backup and restoration of data, and define a process to ensure data integrity upon system recovery.

24.4.7 Safety

There can be many causes of a disaster; and some, such as fire, flood, or hazardous contamination can present a serious threat to personal safety. It must be made clear that, under no circumstances, can personnel charged with disaster recovery tasks enter into a potentially unsafe environment without the express permission of public health and safety officials. The plan should contain detailed information on hazard identification and avoidance and safety procedures.

24.4.8 Security

Disaster breeds confusion, and confusion introduces the opportunity for unauthorized access to valuable property. Access authorization and protocols, including the use of special identification credentials, should be defined and documented.

24.4.9 Test Plan

It is unlikely that recovery operations will succeed in a real disaster if the disaster recovery plan has not been verified and exercised. A test plan and periodic schedule should be proposed.

- The test plan should account for necessary equipment and personnel resources.
- The test schedule should indicate regular intervals for re-testing.

24.4.10 Update Plan

A disaster recovery plan is not a static document. Computing environments constantly change and the plan must track that change to be effective. Disaster recovery plans must be updated whenever system changes that would cause it to become invalid are made. Regardless of system changes, disaster recovery plans must be reviewed annually.

24.5 Compliance

Failure to maintain compliance with this policy may result in the termination of connection to the Worcester State enterprise network. For employees, violations of policy may result in disciplinary action including, but not limited to, permanent loss of access privileges and/or employment termination.