MADISON
AREA | TECHNICAL
COLLEGE

Madison College
Information Protection Standards

Version 1.2
Last Revision Date: July 15, 2015

Table of Contents

Introduction

The Information resources of Madison College are valuable assets and hence must be properly and appropriately protected. Because of the importance of this information, reasonable and appropriate steps must be taken to ensure its:

- *Confidentiality* – ensuring that information is accessible only to those persons authorized to have access – and who need that access in order to perform their duties.
- *Integrity* – safeguarding the accuracy and completeness of information.
- *Availability* – ensuring that information is available to authorized users when it is needed.

The protection of computerized files stored on corporate networks has traditionally been the focus of security specialists. However, information that is stored on a personal computer or other portable device or on a CD, "flash" drive or other media (including paper) must also be protected from harm or unauthorized use or disclosure. Protective measures must also be taken with data as it is being transmitted via E-mail, Fax, or other means.

Proper security controls are essential to maintain the high level of trust that our students – and the community as a whole - have placed in us. This trust can be seriously damaged by even a single incident. Hacker intrusions, web-site defacements, or public disclosures of confidential information could lead to a loss of confidence and/or a degradation of the college's reputation.

Protecting privacy is a major goal of Madison College's Information Security program – but there can be no privacy without security. The college's goal is to provide a level of protection that meets or exceeds the best practices within the realm of Higher Education.

Background

These standards are based upon the "Standard of Good Practice for Information Security" as published by the Information Security Forum (ISF) – an internationally recognized authority (and non-profit organization) in the Risk Management field. The standards are intended to help the college protect its information resources without unduly hampering the legitimate activities that employees are expected to perform as part of their duties. They also take into account any legal or regulatory compliance requirements that the college is obliged to follow.

Document Management

This document is subject to review on an annual (or more frequent if necessary) basis to validate and ensure the relevance and currency of the standards. Significant changes will be reviewed, approved, and endorsed by the college's Executive Team before being implemented.

Any comments or questions regarding these standards, or any suggestions for new standards or revisions to existing ones should be forwarded to the Chief Information Security Officer.

Revision History

Version	Description	Author	Date
1.0	*Initial Publication of Document*	*Bruce Coulter*	*08/15/2012*
1.1	*Communications section revised to remove acknowledgement requirement. Now consistent with HR Employee Handbook requirements.*	*Bruce Coulter*	*11/28/2012*
1.2	*Updated Standard 1.2 Passwords to referenced revised minimum password standard approved in July.*	*Linda Pruss*	*07/15/2015*

Initial Development, Review, and Endorsements

Development, initial review and endorsement of these standards were conducted by a team of individuals appointed by and representing members of the Executive Team. This team was led by Bruce Coulter (Chief Information Security Officer) and included:

Amy Krumenauer – representing Roger Price (Administrative Services)

Carolyn Jarrett – representing Chuck McDowell (Human Resources)

Cigdem Unal – representing Keith Cornille (Student Development)

Lori McRoberts – representing Diane Walleser (Enrollment Management)

Bill Dougherty - representing Diane Walleser (Enrollment Management)

Lori Sebranek – representing Terry Webb (Provost)

Mike Masino – representing Terry Webb (Provost)

All members of the Executive Team have subsequently endorsed and support these standards.

Purpose

These standards have been developed in support of the college's "Information Protection Policy", and provide the "baseline" control measures that all employees of the college are expected to have knowledge of and follow. These measures are required to reduce the likelihood of such problems as inappropriate disclosure of confidential information, identity theft, fraud, embezzlement, sabotage, errors/omissions, or systems unavailability.

Adherence to these standards also helps to ensure that the college is not in violation of any applicable laws or regulations.

Scope

All employees of Madison College – including faculty, staff, (part time and full time), temporary employees, consultants, "casuals", and student help need to have knowledge of and abide by these standards. (Within this document the term "employee" refers to any and all full-time, part-time, or temporary workers or consultants in the employ of college – either directly or indirectly). These standards also apply to any "guest" (i.e., non-student) users of the college's computers, networks, and related resources.

These standards apply to all computing resources (computers, networks, servers, databases, etc.) that are managed by the Technology Services department.

- Specifically "out of scope" are those computing resources that are:
- Provided only in support of the Information Technology instruction area for educational purposes.
- Managed by faculty (or designates) of the Information Technology instructional department.
- Not directly connected to the rest of the college network.

Requests for specific exemptions to any of these standards for any reason may be submitted for consideration by following the "Information Protection Standards Exemption Request" process.

Consequences of Non-Compliance

In order to maintain the high level of trust that our students – and the community –have placed in us, it is essential that employees of Madison College properly protect the information and technology resources that have been entrusted to them. These standards were designed to help achieve that goal – and all employees should know, understand, and abide by them. The college reserves the right to monitor use of its information and technology resources for adherence.

Per the Madison College Information Protection Policy, violation of or non-compliance with any of these standards may result in disciplinary action – up to and including termination of employment.   Any such disciplinary actions will be in accordance with established processes as defined by appropriate collective bargaining agreements and/or other Human Resources policies and procedures as applicable.

In addition, the college reserves the right to take legal action against any employee - past or present – who causes damage to the college's information or technology assets, or who causes a breach of the confidentiality of information by the willful disregard of these standards.

Communications

All employees are expected to know, understand, and abide by these standards. Reminders and clarifications regarding the standards and expectations of employees for abiding by them will be published periodically via the Matters newsletter, the college web pages, or by other means as appropriate.

Topic 1 – Access Control

Principle: Access control arrangements should be established to restrict access to business applications, systems, networks and computing devices by all types of user, who should be assigned specific privileges to restrict them to particular information or systems.

Objective: To ensure that only authorized individuals gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Standard 1.1: User ID's

Each user will have their own User ID to gain access to any Madison College computer system, and is accountable for all actions taken by the User ID assigned to them. Users may only use those ID's which have been assigned to them, or which have been specifically authorized for them to use.

Group, generic, or shared User IDs are only permitted under special circumstances and only with the approval of an appropriate individual willing to assume all responsibility for that shared ID. Such ID's are subject to additional controls and/or access restrictions as appropriate.

Any User ID that has not been used for a period of 90 consecutive days is subject to disablement.

User IDs that have been granted elevated privilege levels (such as "root" in Unix, or "Administrator" on Windows servers) are also subject to additional controls and restrictions.

Purpose

In order to ensure accurate audit trails of actions taken by individuals, it is imperative that a User ID is associated with one and only one person. Without this one-to-one correspondence, individual users cannot be held accountable for their activities performed with a specific User ID.

This standard is also intended to protect against attempts to compromise those IDs that have not been used for extended periods of time. Such IDs are ripe targets, as the rightful owner of the ID is unlikely to notice any compromise of it.

Recommendations and Additional Information

A User ID is what identifies each individual to the college's systems. This means that each individual is responsible for all actions taken under the authority of their ID. The combination of a User ID and password is what gives users access to systems. Because of this, passwords should never be divulged to others (see the Passwords standard).

"Dormant" IDs (those that are not used for long periods of time) are often the targets of hackers, since they know that if they can compromise one of these IDs the rightful owner will probably not notice. To protect against this threat, dormant IDs will be disabled if they are not used for a period of 90 days or more. However, the rightful owner of the ID may reactivate the ID simply by following the Employee Account Activation process, or by contacting the Help Desk for assistance.

It is also recommended that User IDs not be divulged to others – except in those cases where authorized personnel need to know an individual's User ID to assist in problem determination or performance of other administrative duties.

Standard 1.2: Passwords

Passwords associated with computer systems User IDs must be properly managed so as to preserve their integrity and confidentiality. They must never be shared or otherwise revealed to anyone other than the authorized owner of the ID.

Passwords must be constructed so that they can be remembered easily by their legitimate owners, but be hard to guess by others. All passwords must follow the Minimum Password Standard.

To further protect from attack, systems will be configured so that accounts will be disabled after 10 unsuccessful logon attempts. Once disabled, these accounts will be automatically re-enabled after 15 minutes, or upon request – to the Help Desk – by the owner of the ID.

Requests to re-enable a User ID or reset a password will not be honored unless the requestor first properly identifies himself or herself as the legitimate owner of that ID.

Passwords should be changed immediately if it is suspected that it has been compromised.

Purpose

This standard defines the minimum controls that are required to be put in place for all passwords associated with User IDs which have been granted access to Madison College systems. The password is the single most important defense that the college has against unauthorized users and would-be intruders. Ultimately, it is what lies between confidential information and an unauthorized user. It is imperative that all passwords be properly protected and managed.

Recommendations and Additional Information

In addition to never purposely sharing passwords, users must also be cautious of accidentally disclosing them. Passwords should never be spoken out loud (thereby allowing them to be overheard) nor should they be written down and displayed in a prominent place. Generally passwords should never be written down at all – instead they should be created so that they are easy to remember but hard to guess.

If a password must be written down, steps should be taken to properly protect the paper that they are written on. Do not leave the password written on a note attached to your computer or hidden in any obvious place (such as under the keyboard or mouse pad). Ideally, the paper should be kept away from the work area in a secure place.

Here are some helpful hints for creating a strong password that is easy to remember, yet hard to guess:

- Use a mix of letters, numbers, upper/lower case and special characters.
- Don't use your name, user ID, or easily guessed values (like "password", pw, or "default").
- Don't use any words found in a dictionary or any sequence of just numbers.
- Don't use keys that are simply adjacent on the keyboard (like ASDFGH). However, some patterns on the keyboard (like q2w3e4r5t6) can give you a strong password that is still easy to remember. In fact, you could use the same pattern the next time that you change your password – just change the starting character from q to w and you still have a very strong, totally unique, and easy to remember password.
- Think of a phrase that you can remember and then use the first letter of each word of that phrase. Substitute numbers for letters ("2" for "to", "8" for "ate" etc.). For example, "My mother likes to bake cookies for fun!" becomes "Mml2bc4f!".

Proper protection of passwords is the single most effective security measure that can be taken in order to properly protect the systems and confidential information that have been entrusted to an individual.

Any password that is associated with a User ID that has been granted special or elevated administrative privileges is subject to additional password controls and/or requirements that are more stringent than the minimum required controls described in this standard.

Standard 1.3: Computer Privilege Levels

Privileges for users of Madison College’s computer systems and information will be assigned based on job requirements. Only the minimum privileges required to perform the user's specific job function will be allowed.

Under no circumstances will users be given privileges beyond those that are required to adequately perform the duties assigned.

All such privileges assigned will be revoked upon separation from the college. Privilege revocation will coincide with the effective date of the separation.

Purpose

All users of computer systems need access to certain files, applications, and resources in order to perform their assigned duties. But if users are granted privileges beyond what is required to perform these duties, it may give them an increased capability to perform actions that are harmful to the college - some of which may have serious consequences. Such acts may be performed maliciously, but may also be accidental. By restricting privileges and access levels to only what is required by the job function, the likelihood of such damaging actions taking place is greatly reduced.

Recommendations and Additional Information

Determining exactly what privileges any specific user requires can be a difficult task. It can be especially challenging when a new employee is hired, or when an existing employee takes on a new job role.

It is often tempting to simply give these new employees all of the same privileges that were held by the incumbent in the position. Unless clearly-defined permissions appropriate to an employee’s role are defined and enforced, this practice could result in the new employee “inheriting” a set of permissions beyond what is really required for the job being performed. This unnecessary replication of permissions is especially dangerous if permissions that are no longer required are not revoked from employees upon their transfer/promotion to a new position.

Standard 1.4: Protection of Inactive and Unattended Systems

All users must logoff of systems and applications whenever they will not be used for an extended period of time. At a minimum, logoffs should be done at the end of the workday.

When leaving an active workstation unattended, user should first lock the workstation by means of a password-protected screensaver or other method that will prevent unauthorized users from accessing any systems that may be currently active.

All computers provided by the college will be configured to enable a password-protected screen and keyboard lock after a specific inactivity threshold has been reached.

Purpose

This standard is intended to ensure that unauthorized users cannot easily take control of a legitimate user's computer – thereby gaining access to confidential and/or privileged data. Adherence to this standard will help to ensure that data and systems are properly and adequately protected from harm, theft, or misuse.

Recommendations and Additional Information

Follow standard logoff recommendations supplied with each application system that is used.

Some systems may include processes which will automatically end a session after certain thresholds have been reached. These thresholds may be based upon such things as total length of the time the session has been active, total amount of time the session has been inactive, specific times of day that all users must exit a system or other factors unique to that system.

Documentation as to the specific requirements should be included in user documentation accompanying any such systems.

Failure to properly lock a workstation or application when left unattended is a clear violation of this standard. However, the presence of an unlocked, unattended workstation should not be considered an open invitation for other users to use the account that was left unlocked. Such use is considered "unauthorized use" and is a clear violation of the "User ID" standard.

Topic 2 – Personal Use of College Resources

Principle: Employees should be advised of their responsibilities for properly using the college's computing resources – especially such use that is not directly related to conducting business on behalf of the organization.

Objective: To document acceptable and unacceptable activities related to the use of the organization's computing resources for personal reasons.

Standard 2.1: Internet Usage

The Internet access facilities provided by Madison College are the property of the college, and are intended to be used for the purpose of conducting business on behalf of the college.

Some limited use of these Internet access facilities for personal purposes is permitted, provided such use does not:

- Interfere with the employee's ability to perform their expected duties.
- Cause undue slowdowns or performance degradations for other users.
- Expose the college to harm or embarrassment.

The college reserves the right to:

- Block access to any Internet site that may be considered inappropriate or that may pose a risk to the integrity of the college's networks or reputation.
- Monitor usage of the college's Internet access facilities for compliance with this standard.

Purpose

The Internet is an important tool used in the day-to-day operation of the college, but it is also recognized that employees may need to make occasional use of the college's Internet connections for personal reasons. However, if not used properly, this personal use may cause problems for the college and its use of the Internet for business purposes.

Adherence to this standard will help to:

- Protect the college's computers, networks and information from problems which may result from the downloading (intentional or not) or running of computer viruses or other malicious software from infected sites on the Internet.

- Protect the college's Internet access facilities from becoming over-burdened with activity that is not directly related to conducting business.
- Protect the reputation of the college by ensuring that inappropriate or demeaning materials are not obtained using college-supplied Internet access.
- Protect the college from potential legal liability associated with allowing the downloading or distribution of any materials that are copyrighted, pornographic, or legally prohibited.

Recommendations and Additional Information

Usage of the college's Internet access for non-business purposes carries with it many risks, such as:

- Decreased system performance. Legitimate users may experience poor performance or response times due to volumes of activity that serve no legitimate business purpose.
- Computer virus outbreaks. Visits to inappropriate, non-business related Internet sites carries with it an increased risk of infection from computer viruses or other types of malicious software, as these sites are generally not as well controlled as the sites of legitimate businesses.
- Increased volume of unwanted e-mail. Many Internet sites ask for the user's e-mail address in order to facilitate processing. These addresses may then be sold to other marketing firms that use them to send unwanted solicitations (a.k.a. "spam") via e-mail.
- Degradation of reputation. Visits to some sites may result in leaving behind a "footprint" indicating that it was visited by a user of the college's Internet access facilities. Public disclosure of this type of information could damage the college's reputation.

To avoid these problems, users of Madison College's Internet access facilities must refrain from:

- Visiting Internet sites containing pornographic material.
- Visiting sites that promote violence, intolerance, drug/alcohol abuse, criminal activity, or any other objectionable or illegal behavior.
- Visiting sites that allow or promote online gambling.
- Downloading any illegal or illicit materials that are copyrighted or otherwise protected or restricted by law.

Standard 2.2: Storage of Personal Data

The computer data storage resources provided by Madison College are the property of the college, and are intended to be used for the purpose of conducting business on behalf of the college.

Some limited use of these data storage facilities for personal purposes is permitted, with the understanding that:

- Personal data should be stored in a separate and easily identifiable folder so it is easily distinguished from other data.
- No illegal or offensive material may be stored.
- The data stored does not in any way put the system or network at risk.
- Madison College is not responsible for the integrity of the data that is stored and makes no guarantee regarding its availability.
- Data is the property of the college and there is no guarantee that the user will be able to retrieve this data upon transfer, resignation, or termination.
- The size and number of files stored must be limited and not place a burden on bandwidth or back-up programs.

Purpose

This standard defines how authorized individuals may make limited personal use of the college's data storage facilities. Its intent is to protect the college from:

- Harm caused by the introduction of "malware" programs (computer viruses, or other malicious software or utilities).
- Exposure to lawsuits or embarrassment due to the hosting of illegal or offensive materials.
- Slowdowns in the performance of business-related functions, or extra cost of purchasing additional data storage capacity due to the presence of excessive amounts of "personal" data.

Recommendations and Additional Information

Although some limited personal use of the college's data storage facilities is permissible, employees should exhibit good judgment and limit their usage to be in line with the understanding and conditions noted above.

Standard 2.3: Unsupported Software

Computers owned by Madison College are supplied with software that has been researched, tested, licensed and approved by the college. Users of these computers are permitted to install other software, as long as that software:

- Does not cause harm or compromise to any computer or information on the college network.
- Does not interfere with the proper functioning of any other college-owned or sanctioned software.
- Has been properly licensed for use – or does not require a license.
- Is not intended for illegal uses – such as the unlawful downloading or distribution of copyrighted materials.

The college reserves the right to perform an inventory (electronic or otherwise) of all software programs present on any computer owned by the college, and remove any such programs that it deems to be in violation of this standard.

Purpose

This standard is intended to protect computers from harm due to the installation or use of dangerous, unsupported or unsanctioned software programs. It is further intended to help protect Madison College's systems and networks from damage that may arise from malicious software that has been installed on computers that regularly connect to the college's networks.

Adherence to this standard also helps protect the college from any damages which may come as a result of copyright violations perpetrated by users of its computer equipment.

Recommendations and Additional Information

Users should be very selective and cautious about installing any unsanctioned or unsupported software on computers owned by the college. Madison College provides all specific software that is required for users to perform their expected job functions. Installation of any other software may affect the performance and reliability of what is provided.

Some specific examples the dangers of unsupported software include:

- Certain games, utilities and customized screen saver programs have proven to be troublesome to the normal operation of the computer software that has been provided. These programs may change systems settings and configurations that may cause the supplied applications to malfunction.
- Any software designed to allow the computer to participate in a "peer-to-peer" file sharing mode (such as Napster, Morpheus, Kazaa, etc.) is commonly used for the purpose of sharing/downloading music and video files. This type of software has proven to be especially prone to security vulnerabilities - allowing potential

disclosure of confidential data and virus spread. Usage of such software may also put both the user and the college at risk of being in violation of copyright law.

Any free software that is downloadable from the Internet should be considered potentially dangerous. Such software could cause damage to or interfere with the proper operation of legitimate software installed on the computer. In some cases, this malicious software may be used to compromise the computer – making it vulnerable to take-over by unauthorized individuals. These compromised computers could then be used to launch additional attacks against Madison College's networks or against other computers connected to the Internet.

Standard 2.4: Software License Agreements

Licenses for all software products provided by Madison College are owned by the college.

Employees and other authorized users may use the software within the limitations and conditions specified in the licensing agreement. Authorized users may not make or distribute copies of any such software provided by the college, unless doing so is expressly permitted in the terms and conditions of the license.

Purpose

The intent of this standard is to prevent Madison College employees from violating the terms and conditions specified in the End User License Agreements of software provided by the college.

Recommendations and Additional Information

Software is protected under copyright law. Installing single-user licensed software on multiple computers, making copies of software without express permission, or using copyrighted software without a valid license for the version used may all be considered examples of copyright infringement. License infringement can result in loss of use, confiscation of equipment, fines, or other legal action. All employees are responsible for abiding by the terms of use for all software licenses.

Topic 3 - Email

Principle: Email systems should be protected by a combination of policy, awareness, procedural and technical security controls.

Objective: To ensure that email services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimized.

Standard 3.1: E-mail Usage

The e-mail systems and facilities provided by Madison College are the property of the college, and are intended to be used for the purpose of conducting business on behalf of the college.

Some limited use of these facilities for personal purposes is permitted, provided such use does not:

- Interfere with the employee's ability to perform their expected duties.
- Impact the business-related activities of other employees.
- Cause undue slowdowns or performance degradations for other users.
- Expose the college to harm or embarrassment.

All college business conducted via e-mail must be conducted using only those e-mail facilities provided by the college. Personal e-mail accounts (including email services provided by third-parties such as Yahoo, Hotmail, etc.) are not permitted to be used for conducting business on behalf of the college.

The practice of "auto-forwarding" e-mail from a college-supplied e-mail account to a personal e-mail account is expressly prohibited.

Any file containing information that has been classified as "Confidential" (as defined in the "Information Classification and Protection standard") that is included in an email sent outside of the college's email system must be encrypted.

The college reserves the right to monitor its e-mail facilities for adherence to this standard.

Purpose

This standard defines how authorized individuals may use the e-mail facilities provided by Madison College. The intent of this standard is to:

- Protect the college's computers, networks and data from problems which result from inappropriate use of its facilities.
- Protect the college's facilities from becoming over-burdened with activity that is not directly related to conducting business on behalf of the college.
- Protect the reputation of the college by ensuring that inappropriate or demeaning materials are not distributed using facilitates provided by the college.
- Minimize the likelihood of exposure or compromise of information contained within e-mail stored on and processed by the college email facilities.

Recommendations and Additional Information

Although some limited usage of the college's e-mail facilities for non-business purposes is permissible, the storage or transmission of any of the following is prohibited:

- Sexually explicit or suggestive materials.
- Materials that promote the harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.
- Anything that is defamatory, threatening, profane, maliciously offensive, slanderous, or invasive of another person's privacy.

Use of a personal email account (such as those provided by Yahoo, G-mail, etc.) for conducting business on behalf of the college potentially puts the college at risk of:

- Non-compliance with the Wisconsin Open Records Law - This law allows anyone to request information – including copies of email – regarding the college's activities. Use of a personal email account for conducting the college's business could be viewed as a deliberate attempt to circumvent the requirements of this law.
- Compromise of information contained within an email - the college has no means of protecting any email stored on email facilities outside of its control. Any compromise of an external "consumer" email facility could result in the compromise of confidential information contained within any email – or attachments within.

In addition, **unless it is part of a job requirement** as defined and approved by the college, the following activities are prohibited:

- Sending of bulk messages (unsolicited mail to random addresses – sometimes referred to as "spam".)

- Soliciting others for activities unrelated to the college’s business, or for political endorsement purposes.
- Starting or perpetuating “chain” messages (any messages with embedded instructions to re-send it and the instructions to others – including hoax virus warnings).
- Sending messages with executable software attached.

Topic 4 - Information Classification

Principle: An information classification scheme should be established that applies throughout the organization, based on the confidentiality of each piece of information.

Objective: To determine the level of protection that should be applied to particular types of information, thereby preventing unauthorized disclosure.

Standard 4.1: Information Classification and Protection

All information in Madison College's custody must be protected in accordance with the "Data Protection Category" into which it falls. These protective measures must be applied to all information – including both current and backup copies.

For each category defined, the minimum protective measures that must be implemented are as follows:

Data Protection Categories and Protective Measures	
Category	**Minimum Protective Measures**
Unrestricted (Lowest)	No special precautions are required to prevent disclosure of this information. Information may be distributed freely outside the college. However, there will still be controls in place to protect the original/master copies of this information from unauthorized modification, destruction, or loss.

Data Protection Categories and Protective Measures	
Restricted (Medium)	Access is restricted to only those individuals with a "need to know". Release of restricted information outside the college is permitted, but should be done with caution. Release of any information that is requested under the Wisconsin Open Records law may be done only after the request has been reviewed and approved by the college's legal counsel. Such release must be in accordance with all applicable laws and industry regulations When no longer needed, all media containing restricted information must be destroyed or otherwise disposed of in a secure manner in compliance with all applicable document retention policies.
Confidential (Highest)	Access is restricted to only those individuals with a "need to know". Such access is granted only to a limited number of individuals. Papers or "removable media" (such as CD's, diskettes, tapes, flash drives, etc.) containing confidential information must not be left in the open. All such papers and media must be stored in secure areas (such as a locked drawer or file cabinet) when not in use or when left unattended. Portable computing devices (such as a laptop, tablet, or "smartphone") may not be used for long-term (greater than 7 days) storage of any confidential information, unless the information is encrypted. Any confidential information stored on any removable media (such as flash drives, CD's, tapes, etc.) or included in an email sent outside of the college's email system must be encrypted. Confidential information may not be stored on any computing devices belonging to a third party (an individual or organization not employed by or affiliated with the college) unless that party is contractually obligated to protect this information at a level that is comparable to (or greater than) the controls that the college has implemented. Information that is considered confidential is not subject to release under the requirements of the Wisconsin Open Records law. Such information will only be released upon the express written approval of the college's legal counsel.

Data Protection Categories and Protective Measures	
	When no longer needed, all media containing confidential information must be destroyed or otherwise disposed of in a secure manner and in compliance with all applicable document retention policies.

Purpose

This standard helps to ensure that Madison College's information assets are safeguarded in an appropriate manner during its entire lifecycle at the college. Authorized users of information are responsible for applying all measures required to properly protect information from inappropriate disclosure, damage, or alteration.

Adherence to this standard will help to protect the college's information from theft or simple loss. This will help protect the privacy of our students, employees, and others - which in turn will help to protect the college and its reputation.

Recommendations and Additional Information

The Data Protection Category definitions below give a broad overview of the differences between each of the categories discussed in this standard and provide a list of representative information to be considered for protection under this category.

Data Protection Category, Category Definition and Data Considered for Protection

Category	**Definition**	**Data Considered for Protection**
Unrestricted (Lowest)	Information that is freely available to the general public. Disclosure of this information would have no adverse impact on the college.	General information about the college such as campus maps, brochures, handbooks, course catalogs, etc. Faculty, student or staff directory information such as name and email address.
Restricted (Medium)	Information that is only available to specific individuals	Faculty or staff information that is not published or made publicly available, but

Data Protection Category, Category Definition and Data Considered for Protection		
Category	**Definition**	**Data Considered for Protection**
	within Madison College. Access is granted on a "need to know" basis only. Intended to be used primarily by employees of the college for the purpose of conducting business on behalf of the college. Unauthorized disclosure may result in slight to moderate adverse impact, embarrassment, or penalties to the college.	is also not protected by any federal or state privacy laws or industry regulations – such information includes: Employee name Salary Job title Student information that is considered to be "Directory Information" under the Family Educational Rights and Privacy Act (FERPA) – including such things as: • Name • Major field of study • Dates of attendance • Enrollment status • Awards received • Email address Note: if a student has made a formal, written request for their directory information to be withheld (i.e. a "FERPA Hold") that information is then considered "confidential" and must be treated accordingly. Information related to the college's contractual agreements or other obligations. Financial and budgetary reports.

Data Protection Category, Category Definition and Data Considered for Protection

Category	**Definition**	**Data Considered for Protection**
Confidential (Highest)	Information that is only available to very limited subsets of individuals within Madison College. Access is granted on a "need to know" basis only. Unauthorized disclosure is likely to result in a significant adverse impact, embarrassment, or penalties to the college. Disclosure may cause a high risk for identity theft, and/or be in violation of federal or state privacy laws or applicable industry regulations. Disclosure may aid malicious outsiders in developing computerized attacks against the college networks and bypass or defeat the automated defensive controls in place.	Any personal Information that is protected by Federal or state privacy laws or by applicable industry regulations – including (but not limited to): • Social security number, or national ID number • Medical information, including ability to work information and absences due to illness records • Driver's license number • Date of birth • Bank account or credit card numbers • Results of background or criminal checks • Home address Student information that is protected under the Family Educational Rights and Privacy Act (FERPA). (That is, any student information that is not considered to be "Directory Information"). Examples include individual student information pertaining to: • Student ID Number

Data Protection Category, Category Definition and Data Considered for Protection		
Category	**Definition**	**Data Considered for Protection**
		• Transcripts and Grades • Counseling sessions • Disciplinary actions • Financial Aid or Grants Any student "Directory Information" for students who have made a formal, written request for that information to be withheld. (i.e. a "FERPA Hold". Such students are often referred to as "Buckley" students). Personnel records including details of performance reviews, disciplinary actions taken, counseling sessions provided, etc. Information related to measures employed by the college to protect its network or data – such as passwords, details of internal security controls, firewall settings, results of risk or vulnerability evaluations, etc.

It is important to remember that all media containing confidential and/or restricted information must be properly destroyed before it is discarded. All paper documents must be shredded before disposal. Certain magnetic media (diskettes, tapes, CD's) may also be shredded – depending upon the capacity of the shredding machine being used. If shredding of such media is not feasible, other means of destroying the media or otherwise rendering the information on the media unreadable – such as running a powerful magnet over tapes or breaking CD's into multiple pieces – are also acceptable.

Topic 5 - Malware

Principle: All individuals who have access to information and systems of the organization should be made aware of the risks from malware, and the actions required minimizing those risks.

Objective: To ensure all relevant individuals understand the key elements of malware protection, why it is needed, and helps to keep the impact of malware to a minimum.

Standard 5.1: Computer Virus Protection

Users must not intentionally introduce any computer code designed to hinder the performance of or access to any Madison College computer system, network or information. (E.g. computer viruses, worms, Trojan horses and other malicious software).

All workstations are equipped with up-to-date anti-virus software. To ensure its effectiveness, users must be sure to:

- Never attempt to purposely disable or uninstall the anti-virus software provided, nor interfere with any updates to it.
- Report any problem with either the detection or eradication of viruses.
- Immediately comply with any and all directives issued by authorized support personnel regarding ways to either repair damage from or mitigate risk of a computer virus infection.
- Not attempt to install any other anti-virus software.

Users must NOT circulate virus or malicious software warnings to other individuals, especially via the Madison College e-mail system.

Purpose

This standard has been established to ensure that proper technical and business practices are in place to identify and eliminate computer virus infections from Madison College computer systems.

Recommendations and Additional Information

All Madison College computer systems are protected from computer viruses, worms, Trojan horses and other malicious software (a.k.a. “malware”). This protection involves the use of specialized anti-virus software that scans files for the presence of such malware. The software has proven to be very effective at detecting and stopping virus infections, but no anti-virus software can ever be considered "foolproof". For this reason, all computer users should take some additional precautions to help further protect their computers from virus infection:

- Be suspicious of any unexpected e-mail containing file attachments or links to external web pages.   Opening these attachments or clicking on such links may cause malware to be downloaded and installed on your computer.
- Be cautious when downloading files from the Internet. Most reputable businesses include anti-virus measures on their websites, but very few will make guarantees that downloads from their site are "virus free".

Installation of other anti-virus software not supplied or sanctioned by Madison College may cause other problems for the user – including system conflicts, degradation of performance and unexpected computer failures. For this reason, users should NOT attempt to install any other anti-virus software.

Users are also advised to be skeptical of any e-mail or other announcements that may be received warning of new viruses and the dire consequences of infection by them. Most such warnings are simply hoaxes designed to spread fear and panic. They will often implore the recipient to pass the warning on to everyone they know – thus flooding e-mail systems with bogus warnings and overburdening e-mail systems to the point of failure. If such a warning is received, it may be forwarded to the Madison College Help Desk for review and verification.   However, in most cases these warnings will be hoaxes and can simply be ignored. Under no circumstances should such warnings be forwarded to others.

Topic 6 - Information Security Incident Management

Principle: Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective: To identify and resolve information security incidents quickly and effectively, minimize their business impact and reduce the risk of similar incidents occurring.

Standard 6.1: Reporting Security Incidents

All information security incidents (such as exposure of confidential information, equipment loss or theft, etc.) or violations of any policy or standard designed to protect the college's information or technical resources must be reported immediately. Suspicious incidents or behaviors should also be reported.

In addition, tampering with any evidence related to an information security incident (suspected or actual) is prohibited.

Employees should report such incidents directly to the Help Desk, or their immediate supervisor.

Purpose

The purpose of this standard is to minimize loss and exposure to the college from information security incidents. By gathering reports of actual or suspected incidents, a larger pattern of behavior may be detected which may be indicative of malicious activity. Delays in reporting could result in additional losses for the college.

Recommendations and Additional Information

Information security incidents that must be immediately reported include violations of existing protection standards and any case of equipment loss or theft. Other activities or incidents that seem suspicious or questionable should also be reported.

Of special interest is any suspected use of "social engineering" – that is, attempts to use psychological tricks to obtain information to gain access to a computer system. Most often such social engineering is perpetrated by phone, but the use of other methods such as email and malicious web sites are on the rise. The caller may identify themselves as a member of the Help Desk staff, or as an assistant to a high-ranking executive and ask that you provide them with information (possibly even including User IDs and passwords), which then may be used to attack, or otherwise compromise systems.

Information about other employees or details about internal systems networks or applications should never be given out unless the identity of the requestor has been verified, and it has been determined that the requestor has a valid need for and is authorized to receive the information. Any suspected use of social engineering techniques is considered a suspicious behavior, and should be reported immediately.

Topic 7 – Computer and Network Installations

Principle: Computer system, network, and telecommunications installations (e.g. data centers) should be designed to cope with current and predicated information processing requirements, and be protected using a range of built-in security controls.

Objective: To ensure computer system, network, and telecommunications installations can meet the security requirements of the critical business applications they support (i.e. protect against the compromise of confidentiality, integrity, and availability of information they process.

Standard 7.1: Internal Network Access

Computer hardware (including desktops and laptops) that is not owned, managed, installed or approved by Madison College or its authorized service providers are restricted from being directly connected to the Madison College internal computer network.

The college reserves the right to disable or remove any computer hardware that is found to be in violation of this standard.

Purpose

This standard is meant to protect Madison College networks and data from compromise or damage due to improperly configured or managed computer hardware that is directly connected to the college's internal network. If unsupported or improperly configured devices were allowed to connect to the network, many security vulnerabilities and other problems could be introduced - including:

- The spread of computer viruses or other malicious software.
- Compromise of the college's network due to the presence of "hacking "tools or software on an unsupported device.

Note that this standard prohibits unapproved personally-owned computing devices from directly connecting to the internal college network (via Ethernet cable, wireless, or other means), but it does NOT restrict the use of such devices from accessing those services or applications that are provided via the college's public website. These services and applications have been specifically designed for this type of access – and include additional protective measures (such as firewalls, security "zones", etc.). Such services include:

- The college's Wireless Access services for connecting to the Internet.
- All parts of the Madison College Web page.
- Email (via Outlook Web Access).
- File Access (including "Home" and "Share" drive access via Fileway).
- PeopleSoft (via the "MyMadisonCollege" portal).
- Blackboard

Recommendations and Additional Information

Personally-owned devices (or other devices not owned or managed by the college) are not allowed to be directly connected to the college's internal network. This access restriction is enforced via technological controls. However, users of such devices may still use them to access the Internet (via the college's Internet connections - wired or wireless) and then access any services provided by the college via its publicly-facing Internet page.

If it is determined that a specific department or area requires new computer hardware that must be directly connected to the internal network, the procurement, configuration and installation of the hardware must be coordinated with appropriate personnel authorized to perform these functions. Doing so will ensure that the hardware is installed and configured so that it is afforded all the same protections as any other existing device. It will also help to keep other devices within the college protected from a variety of security vulnerabilities.

Standard 7.2: Unsupported Network Hardware

Network hardware (such as wireless access points, routers, switches, servers, etc.) directly connected to the Madison College internal computer network may only be installed by authorized Madison College personnel – or by external service providers who are under contract and have been expressly authorized by Madison College to provide this service.

The college reserves the right to disable or remove any network hardware that is found to be in violation of this standard.

Purpose

This standard is meant to protect Madison College networks and data from compromise or damage due to improperly configured or managed network devices. When unsupported or improperly configured devices are connected to the network, many security vulnerabilities and other problems may be introduced - including:

- Severe performance degradation of the entire network.
- Inability to properly deploy security patches and usability enhancements.
- Decreased capability to deploy anti-virus updates in a timely and efficient manner.
- Compromise of the college's networks and data by unauthorized outsiders.
- Faulty or incomplete inventory reports.

Recommendations and Additional Information

If it is determined that a specific department or area requires additional network hardware, the procurement, configuration and installation of the hardware must be coordinated with appropriate personnel authorized to perform these functions. Doing so will ensure that the hardware is installed and configured so that it is afforded all the same protections as any other network device. It will also help to keep other devices within the college protected from a variety of security vulnerabilities:

- If security patches cannot be properly deployed due to the presence of an unsupported device, other workstations and network hardware connected to that device may also be affected. Unless the network hardware is installed and configured properly, anti-virus updates may not be able to be distributed. This could result in an increased likelihood of infection by computer viruses or other malicious software programs.
- Improperly installed or configured wireless LANs and routers are especially prone to compromise by outsiders. Such compromise could also lead to severe network performance degradation due to increased traffic stemming from unauthorized external sources.
- Improperly configured devices could cause automated inventories of software, workstations, servers, and other devices to be reported incorrectly. This in turn

could lead to an inability to recognize and react to security threats and vulnerabilities that may go undetected. It could also cause the college to be in violation of software licensing agreements with its software vendors.

Standard 7.3: Wireless Network Access

The college's wireless access infrastructure (providing access to both the Internet and the college's internal network) is intended for use only by authorized individuals - including students, faculty, staff, and authorized guests.   Any user of these wireless capabilities must first identify and authenticate themselves - by means of a User ID and password, or other authentication mechanism provided by the college.

Unauthenticated access to the wireless infrastructure is not permitted.

Purpose

This standard is meant to protect Madison College from problems that may arise from the unauthorized and/or "anonymous" use of its wireless network access – especially the direct Internet access that is provided.   Requiring authentication before allowing access will help to:

- Ensure that only authorized users – who are aware of and have agreed to abide by - the college's policies and standards are using the Internet access facilities provided.
- Protect the college's Internet access facilities from becoming over-burdened with activity that is not related to any legitimate business of the college – or the academic activities of its students. Such activity may have an adverse effect on legitimate and authorized use of these facilities.
- Enable the college to monitor use of its Internet access facilities for adherence to the policies/standards of the college – as well as adherence to any applicable legal and regulatory requirements regarding the downloading or distribution of copyrighted material, pornography or other inappropriate materials.

Recommendations and Additional Information

Wireless access to the Internet and the college's network is provided as a convenience and productivity booster to all authorized users. However the college must be very careful to protect these access facilities from harm or abuse by those unauthorized to use these facilities so that authorized users are not adversely impacted.

The authentication requirement is only one of many protective measures that the Technology Services staff has put in place to provide this protection.

Standard 7.4: Remote Access

Access to the internal components of Madison College's technical infrastructure (that is, any component or service that is not directly accessible via links provided on the college's publicly facing web-pages) from any off-campus location is allowed only via tools and technologies provided by the college specifically for this purpose.

Any such access requires the use of "Two-Factor Authentication" technology supplied by the college.

Purpose

The purpose of this standard is to protect Madison College systems and networks from damage or compromise that could be inflicted as a result of using unsupported or insecure remote access software or utilities. It is further intended to help protect computers used by Madison College employees from harm that could be caused by the use of such software.

Recommendations and Additional Information

A variety of tools and services are available which provide capabilities to remotely access and/or control other computers connected to the Internet. Although many of these tools also include some basic security mechanisms intended to protect against unauthorized usage, their use poses a significant risk to the security of computers exposed to them, and to any network to which the exposed computers are connected. These risks include:

- The ability to more easily propagate computer viruses and other malicious software.
- The capability to intercept passwords and other confidential data being passed through unsecured Internet connections.
- Capturing passwords or other confidential data via the use of keystroke logging software which may be installed on computers used in public places or "Cyber Cafes".

Using remote control software to remotely access computers directly connected to the colleges' internal network can be especially dangerous, since these computers – if compromised - could potentially be used to further compromise other computers or data hosted on the college network.

For these reasons, any such use of remote control software not specifically provided and supported by Madison College is prohibited.

Standard 7.5: Physical Protection of Hardware and Networks

All hardware used to support the college computing infrastructure (including servers, routers, switches, firewalls, telecommunications equipment, etc.) will be housed in secure areas to protect them from unauthorized access, attack, or accidental damage.

Access to these secure areas will be allowed only for those personnel who are responsible for the maintenance and/or support of this equipment.

Purpose

This standard is meant to protect Madison College networks, data, and other critical facilities from physical harm. By housing this equipment in secure areas and restricting access to these areas, the likelihood of such damage occurring (either from intentional or accidental causes) is greatly reduced.

Recommendations and Additional Information

Access to secure areas hosting the college's computing infrastructure and equipment needs to be severely restricted so as to provide the highest level of protection possible. This protection in turn will help to decrease the likelihood of:

- Outages experienced by all uses of the college computing infrastructure.
- Compromise of the confidentiality or integrity of the data hosted with the college computing environment.

Outside contractors/consultants may require access to these areas on an occasional and temporary basis in order to perform their duties for the college. However, anyone requiring this access should gain permission for the access prior to their visit – or else be escorted by 1 or more authorized personnel while they are inside of any secured areas.

Topic 8 – Mobile Devices

Principle: Mobile devices (including laptops, netbooks and consumer devices such as tablets and smartphones) should be configured to function as required, protect against unauthorized disclosure of information and help prevent loss or theft.

Objective: To ensure mobile devices do not compromise the security of information stored on them or processed by them, and prevents unauthorized access to information in the event they are lost or stolen.

Standard 8.1: Protection of Portable Computing Devices

All portable computing devices provided to employees by Madison College (such as laptop, notebook, tablet, handheld computers, etc.) must be both physically and logically protected from loss, theft, or data compromise.

Users must be sure their devices are physically secured whenever left unattended. This can be accomplished by such means as a locking docking station, a properly secured cable lock, or storage in a locked drawer or file cabinet. Portable computing devices must never be left unattended in public places.

In addition, all such devices must be configured so that a password (or similar control) is required to logically "unlock" the device upon initial power-up. Devices must also be configured to "lock" after no more than 15 minutes of inactivity – with entry of the appropriate password/control required to unlock it.

Incidents of lost or stolen computing devices must be reported immediately.

Purpose

The purpose of this standard is to ensure that computer system hardware and data stored on such devices are properly and adequately protected from harm, theft, or misuse.

Recommendations and Additional Information

All personnel who are in possession of a portable computing device provided by Madison College should follow these guidelines:

- Do not leave any such device unattended in your office, work area, or public space unless it is properly secured via a cable lock, placed in a locked cabinet/drawer, or physically secured by some other mechanism.
- When using a cable lock, be sure that the cable is locked to a fixed object that is not easily moved, lifted, or stolen along with the computer.

When Traveling:

- Carry your device in a padded, protective bag. A carrying bag that is not immediately recognizable as containing a portable computing device is advisable. Any potential thief will be more likely to target those bags that are obviously holding a computing device. Placing the padded, protective case for the computer within another briefcase or athletic bag is a good way to "disguise" your device.
- Do not "check" your device through airports as luggage. The risk of theft or damage far outweighs any benefits.
- Be especially alert while waiting in lines at security checkpoints in airports, as they can be prime times for a thief to cause a distraction while an accomplice steals your device.
- Never leave your portable computing device unattended in a public place (such as restaurants, hotel lobbies, airport waiting areas, etc.).
- If you must leave your device in an unattended car, be sure that the car is locked and that the device is stored out of sight - preferably in the trunk.
- Use a cable lock if you must leave your device unattended and exposed in a hotel room. Be sure that it is securely locked to a fixed, hard to move object within the room. An alternative is to store the device in an in-room safe or lockable drawer.

The use of a “power-on” password coupled with an automatic inactivity timer (set to “lock” the device after no more than 15 minutes of inactivity) will greatly help to lessen the likelihood of compromise of a device that is lost or stolen.

Standard 8.2: Personally Owned Consumer Devices

Personally-owned consumer devices (such as smartphones, tablets, laptops, etc.) may be used for conducting business on behalf of the college. Any files used in support of conducting that business may be stored on the personally owned device, provided the following conditions are met:

- Any such file is a copy. No "original" versions of any files may be stored on any device not owned or managed by the college.
- The copy is protected at substantially the same – or greater – levels as the original.
- The copy may be destroyed without causing any undue harm to the college.
- The individual assumes all responsibility and accountability for properly protecting the files stored or processed on the device.
- Long-term (greater than 7 days) storage of any information that has been classified as "Confidential" - as defined in the "Information Classification and Protection" standard – is allowed only if that information is encrypted.

By using a personally-owned device for storing information belonging to the college – including any synchronized email – the user implicitly understands and agrees to the following:

- All college-owned information stored on the device – including the contents of any email addressed to or sent from the owner's college e-mail address – remains the property of the college.
- The device will be configured so that college email will only be kept on the device for a maximum of 7 days.
- The device will be physically protected from loss or theft.
- The device will be configured so that a password (or similar control) is required to logically "unlock" the device upon initial power-up. Devices must also be configured to "lock" after no more than 15 minutes of inactivity – with entry of the appropriate password/control required to unlock it.
- Any loss or theft of the device will be reported immediately.
- All copies of college email or other information owned by the college will be promptly removed from the device upon the employee's termination of employment with the college.

In addition, the college reserves the right to:

- Audit, inspect, or confiscate any device suspected of being in violation of this standard.
- Remotely "wipe" all information from the device in the event of a security incident (including the loss or theft of the device) or upon termination of the owner's employment with the college.

Purpose

This standard defines how personally–owned consumer devices may be used for conducting business on behalf of the college. It defines the minimum level of controls that must be put in place to properly protect the college's information.

If proper controls are not in place, the loss or theft of any such device could result in compromised information and the compromise of a college email account. Such accounts could subsequently be used to read/monitor the owner's email, but also to send inappropriate, threatening, or otherwise unwanted email from the owner's email address.

Recommendations and Additional Information

Physical protection of any device is the best defense against compromise. Owners of these devices should take care not to leave them unattended – especially in any public areas. The use of a "power-on" password coupled with an automatic inactivity timer (set to "lock" the device after no more than 15 minutes of inactivity) will greatly help to lessen the likelihood of compromise of a device that is lost or stolen.

In the event of the loss or theft of a device it is critical that the device be "wiped" as soon as possible so as to prevent the compromise of any information or email accounts configured on the device. The Help Desk should be contacted immediately upon discovery of any such or loss or theft, as they can guide the owner thru the process of performing this process.

Depending on the type of device used, this wipe process may be done by the individual owner, or – in the case of some smartphones - may need to be performed by the device's service provider. If the device was configured to synchronize with the owner's college email account, it may also be "wiped" by using the facility currently provided within Outlook Web Access.

Appendix A – Cross-Reference to ISF Standards

ID	Standard Name	Related ISF Standards of Good Practice
1.1	**User ID's**	**CF6.1.2** **CF6.1.7** **CF6.1.8** **CF6.2.1**
1.2	**Passwords**	**CF6.4.2** **CF6.4.3** **CF6.4.4** **CF6.7.2**
1.3	**Computer Privilege Levels**	**CF2.1.4**
1.4	**Protection of Inactive and Unattended Systems**	**CF14.1.5** **CF14.2.5**
2.1	**Internet Usage**	**CF1.1.6**
2.2	**Storage of Personal Data**	**CF1.1.6**
2.3	**Unsupported Software**	**CF1.1.6**
2.4	**Software License Agreements**	**CF1.1.3**
3.1	**E-mail Usage**	**CF1.1.6** **CF15.1.2** **CF15.1.4** **CF15.1.9**
4.1	**Information Classification and Protection**	**CF1.1.3** **CF3.1.1** **CF3.1.2** **CF3.1.3** **CF3.1.4** **CF14.2.6**
5.1	**Computer Virus Protection**	**CF10.2.1** **CF10.2.2** **CF10.2.3** **CF15.1.9** **CF14.2.5**

Continued…

6.1	Reporting Security Incidents	CF11.1.3 CF11.1.4
7.1	Internal Network Access	CF9.3.1 CF9.3.4 CF9.3.10
7.2	Unsupported Network Hardware	CF9.3.4 CF9.3.10
7.3	Wireless Network Access	CF9.6.2 CF9.6.5
7.4	Remote Access	CF6.1.4 CF6.5.1 CF6.1.7 CF6.2.1 CF9.3.6 CF9.3.8
7.5	Physical Protection of Hardware and Networks	CF7.2.6 CF19.1.2 CF19.1.8
8.1	Protection of Portable Computing Devices	CF14.1.1 CF14.1.2 CF14.1.6
8.2	Personally Owned Consumer Devices	CF14.5.1 CF14.5.3 CF14.5.4 CF14.5.5 CF14.5.6