

THE
UNIVERSITY
OF RHODE ISLAND

THINK BIG  WE DO™

Information Technology Services
Office of Information Security



Information Security Policy

Table of Contents

<i>Introduction</i> _____	4
<i>Scope</i> _____	5
<i>Roles and Responsibilities</i> _____	5
<i>Compliance</i> _____	5
Internet Usage Policy _____	5
Employee Monitoring _____	9
Employee Compliance Agreement _____	10
Information Classification and Sensitivity Policy _____	13
Administrative Safeguards _____	15
Security Management _____	16
IT Usage Authorization _____	18
Data Backups and Recovery _____	20
External Party Security _____	21
Information Security Activity Review _____	23
Incident Handling and Response _____	24
Violation Reporting _____	26
Information Disposal _____	27
Training and Awareness _____	28
Physical Safeguards _____	29
Device and Media Controls _____	30
Computer/Network Physical Security _____	31
Facility Controls _____	33
Technical Safeguards _____	36
Audit Policy _____	37

Transmission Security _____ 38
Encryption _____ 40
Access Controls _____ 41
Computer/Network Security _____ 45

DRAFT

Introduction

The University of Rhode Island is the State's public learner-centered research university. It is a community joined in a common quest for knowledge. The University is committed to enriching the lives of its students through its land, sea, and urban grant traditions. URI is the only public institution in Rhode Island offering undergraduate, graduate, and professional students the distinctive educational opportunities of a major research university. Our undergraduate, graduate, and professional education, research, and outreach serve Rhode Island and beyond. Students, faculty, staff, and alumni are united in one common purpose: to learn and lead together.

Embracing Rhode Island's heritage of independent thought, we value:

- Creativity and Scholarship
- Diversity, Fairness, and Respect
- Engaged Learning and Civic Involvement
- Intellectual and Ethical Leadership

Information and information systems are critical and vitally important to The University of Rhode Island's assets. Without reliable and properly secured information and information systems, The University of Rhode Island's information resources would be at risk. Likewise, the preservation and enhancement of The University of Rhode Island's reputation is directly linked to the way in which both information and information systems are managed. Maintaining an adequate level of security is one of several important aspects of both information management and information systems management. The purpose of these policies is to establish management direction, procedures, and requirements to ensure the appropriate protection of The University of Rhode Island informational assets.

These policies have been grouped as follows:

- ***Information Sensitivity and Classification:*** An individual policy which defines classifications levels of data and explains who may classify data.
- ***Administrative Security Controls:*** A set of policies that pertain to the non-technical controls, such as authorization to use systems, account management, privileged user, data backup and recovery, etc...
- ***Physical/Environmental Security Controls:*** A set of policies that pertain to the physical and environmental protection of information and information system resources.
- ***Technical Security Controls:*** A set of policies that define key technical security controls and provide guidance and standards for using these controls. Examples include user identification and authentication, access controls, and malicious code protection.

Scope

These policies apply to all employees, contractors, consultants, temporaries, guests, volunteers and other workers at The University of Rhode Island, including those workers affiliated with third parties who access The University of Rhode Island's computer networks. Throughout these policies, the term "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer data communication systems and informational assets in all forms owned by and/or administered by The University of Rhode Island.

Roles and Responsibilities

The University of Rhode Island has established the position of Associate Director of Information Security. The title "Information Security Officer" will be used to refer to the Associate Director of Information Security. The individual named to this position has been granted the authority to oversee all ongoing activities related to the development, implementation, maintenance, and enforcement of all Information Security policies and procedures contained herein covering the security of the University's Information systems and assets. The responsibilities of this position also require the individual maintain a current knowledge of applicable federal and state security laws and be the lead individual from The University of Rhode Island in any security investigation, be they internal or external.

Compliance

As information systems become increasingly distributed (through mobile computing, desktop computing, Colleges, Remote VPN Access, etc.), users are increasingly placed in a position where they must handle information security matters that they did not handle previously. Therefore, every worker at The University of Rhode Island -- no matter what their status (employee, contractor, consultant, temporary, etc.) -- must comply with the information security policies found in this and related information security documents. Violations of this policy and other security related documents shall be handled consistent with University disciplinary procedures applicable to the relevant person.

Internet Usage Policy

Purpose

The intent of this policy is to establish guidelines for the proper use of The University of Rhode Island supplied email and Internet access. The University of Rhode Island provides e-mail and Internet access to its employees to assist and facilitate business communications and work-related

research. In an effort to ensure the highest level of professionalism and appropriate use of University of Rhode Island Resources, we require all employees to acknowledge our Internet and e-mail policies. This policy is based on common sense and is not meant to be exhaustive. Interpretation of this policy is at the discretion of The University of Rhode Island. Violations of this policy and other security related documents shall be handled consistent with University disciplinary procedures applicable to the relevant person.

University Property

As a productivity enhancement tool, The University of Rhode Island encourages the business use of electronic communications (notably the Internet, voice mail, electronic mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of The University of Rhode Island.

Authorized Usage

Electronic communications systems generally must be used only for business activities.

Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any University activity. Users are forbidden from using electronic communication systems for private business activities, or amusement/entertainment purposes. Employees are reminded that the use of University resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Only authorized employees may communicate on the Internet (or elsewhere) on behalf of The University of Rhode Island. Employees may not express opinions or personal views in any manner that may allow them to be misconstrued as being those of The University of Rhode Island. Employees may not state their affiliation with The University of Rhode Island on the Internet unless required as part of their assigned duties. Keep in mind that when using The University of Rhode Island's e-mail system or Internet access, the recipient(s) might view such correspondence, opinion, information, registration or subscription as authorized by The University of Rhode Island, similar to using The University of Rhode Island Stationery or letterhead.

User Identity

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. The user name, electronic mail address, institutional

affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

No Default Protection

Employees are reminded that The University of Rhode Island electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communication systems, encryption or similar technologies to protect the data must be employed.

Respecting Privacy Rights

Except as otherwise specifically provided, employees may not intercept, disclose or assist in intercepting or disclosing, electronic communications. The University of Rhode Island is committed to respecting the rights of its employees, including their reasonable expectation of privacy. The University of Rhode Island also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

No Guaranteed Message Privacy

The University of Rhode Island cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, electronic communications can be accessed by others in accordance with this policy.

Regular Monitoring

It is the policy of The University of Rhode Island to periodically monitor the content of electronic communications. The content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that The University of Rhode Island will from time to time examine the content of electronic communications.

Inappropriate Electronic Communications

Inappropriate Internet / e-mail use includes but is not limited to:

- Unauthorized transmission of any University of Rhode Island confidential or proprietary information, including, without limitation, confidential information, code or data, or other material covered under The University of Rhode Island policies. In addition, be particularly cautious when transmitting confidential or proprietary information, even when authorized.

- Transmitting personal conversations as to excessively interfere with your professional obligations to The University of Rhode Island, or inappropriate usage, i.e., chat rooms, instant messaging, bulletin boards, jokes, chain letters, etc.; such determination will be at The University of Rhode Island's sole discretion.
- Accessing any web site for which you are not authorized;
- Transmitting harassing, obscene, racial, gender-specific, offensive or unprofessional messages, or any derogatory comments relating to age, race, religion, color, sex, sexual orientation, or other characteristics specified by applicable law;
- Accessing any web site which could be reasonably considered to be sexually or racially offensive or discriminatory in any manner;
- Displaying, downloading or distributing material which could be reasonably considered to be sexually, racially, religiously, or otherwise offensive material.

Should these stated or other prohibited uses cause an unproductive or hostile environment, please discuss them with your immediate supervisor or another member of management with whom you feel comfortable. Appropriate action will be taken as soon as reasonably possible. If you have any questions regarding the interpretation of this policy, please contact the Director of Human Resources.

Downloading of Software

Any software or other material downloaded onto University of Rhode Island Computers may be used only in ways consistent with the licenses and copyrights of the vendors, authors and owners of the material.

Testing Controls

Workers must not "test the doors" (probe) security mechanisms at either The University of Rhode Island or other Internet sites unless they have first obtained permission from the Information Security Officer. If workers probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity. Likewise, both the possession and the usage of tools for cracking information security (such as Nessus or Metasploit) is prohibited without the advance permission of the Information Security Officer.

Employee Monitoring

Purpose

The purpose of this policy is to provide advance notice to University of Rhode Island employees of the University's intent and ability to perform electronic monitoring of employee activities within University premises or when engaged in electronic communications over University systems. "Electronic monitoring" means the collection of information within University of Rhode Island facilities concerning an employee's activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photo electronic or photo-optical systems, but not including the collection of information for security purposes or collection of information prohibited under state or federal law.

Monitoring

Employees are hereby notified that when The University of Rhode Island has reasonable grounds to believe that an employee is engaged in conduct which (i) violates the law, (ii) violates the legal rights of the University or violates the legal rights of University of Rhode Island employees, or (iii) creates a hostile workplace environment, and electronic monitoring may produce evidence of this misconduct, The University of Rhode Island may conduct electronic monitoring of the employee in question without prior written notice.

Enforcement

The University of Rhode Island CIO and Information Security Officer have access to all data stored on University of Rhode Island owned computers and is authorized as necessary to monitor compliance with its policies and to conduct any electronic monitoring. The Information Security Officer will review alleged violations of University policies in the use of University of Rhode Island Systems on a case-by-case basis. Clear violations of established policies may result in termination of the access to University resources for the person(s) at fault. In addition, The University of Rhode Island Information Security Officer shall refer all violations of established policies for possible disciplinary action to the appropriate supervisory authority. All supervisory authorities are required to enforce established policies and are authorized to issue appropriate discipline including possible discharge from employment for violations of established policies. Violations of law in the use of University of Rhode Island Computer network are subject to possible criminal sanctions will be referred to the appropriate State and/or Federal agency.

Employee Compliance Agreement

A signed paper copy of this form must be submitted with all requests for (1) authorization of a new user-ID, (2) authorization of a change in privileges associated with an existing user-ID, or (3) periodic reauthorization of an existing user-ID. University of Rhode Island Management will not accept modifications to the terms and conditions of this agreement.

User's Printed Name: _____

User's Department: _____

User's Telephone Number: _____

User's Access Type: _____

I, the user, understand that I have been granted access to proprietary, confidential University data in order to perform my function within the University.

I agree to take all reasonable precautions to assure that University of Rhode Island internal information, or information which has been entrusted to The University of Rhode Island by third parties (such as customers or participants), will not be disclosed to unauthorized persons. At the end of my employment or contract with The University of Rhode Island, I agree to return to The University of Rhode Island all information to which I have had access in order to do my job. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal University of Rhode Island Manager who is the designated information owner.

I have access to a copy of the University of Rhode Island Information Security Policies, I have read and understand these materials, and I understand how they impact my job. As a condition of continued employment at The University of Rhode Island, I agree to abide by these information security policies. I understand that non-compliance will be cause for disciplinary action up to and

including system privilege revocation, dismissal from The University of Rhode Island, as well as criminal or civil penalties.

I agree to choose a difficult-to-guess password as described in The University of Rhode Island Information Security Policies document, I agree not to share this password with others, and I agree not to write the password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the Information Security Officer or my department manager.

User Signature & Date: _____

For Department Heads Only

I, the manager, understand that the user identified within this document has been granted the following types of access to University of Rhode Island proprietary, confidential data:

Manager's Printed Name: _____

Manager's Department: _____

Manager's Telephone Number: _____

Manager's Signature & Date: _____

Information Classification and Sensitivity Policy

Purpose

Information is important and pervasive to University of Rhode Island Business. The purpose of this policy is to describe what The University of Rhode Island established data classification levels are and the proper methods for handling such information.

Scope

This policy applies to all information within The University of Rhode Island's control, regardless of its format, oral, electronic, or printed. All workers have an important role to play as well as a responsibility to protect the information entrusted to their care. All workers are expected to familiarize themselves with this policy and to consistently use it in their business activities.

Information Stewards

All information possessed by or used by a particular organizational unit within The University of Rhode Island must have a designated steward. Information stewards are responsible for assigning appropriate sensitivity classifications as defined immediately below.

Data Classifications

Restricted

This classification applies to business information that is designated for Senior Managers or designees. Senior Managers or designees are the designated Information Stewards of this information classification. Examples of such information are: Financial Information, Personal Health Information and sensitive human resource information such as employee investigations. This information must be labeled. Printed copies must be accounted for. Computer files must be password protected and/or encrypted. Documents must be shredded when discarded.

Classified

This classification applies to information that is intended for use within The University of Rhode Island. Its unauthorized disclosure could adversely impact The University of Rhode Island, its business partners, its employees, and/or its customers. Information that some people would consider to be private is included in this classification. Examples include employee personnel records, strategic alliance agreements, unpublished market research, passwords, and internal audit reports.

Public

This classification applies to information that has been explicitly approved by management or public relations for release to the public. By definition, there is no such thing as unauthorized

disclosure of this information and it may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Classification Modifications

Only identified information stewards may reclassify information. This reclassification process must be documented stating the type of information to be reclassified, purpose of reclassification, and contain the authorized signature of the information steward.

DRAFT

Administrative Safeguards

Introduction

This section of the policy manual pertains to non-technical controls put in place to ensure the security of University of Rhode Island Information assets.

Areas addressed within this section include:

- Security Management
- Data Backup/Recovery
- External Party Security
- Incident Handling/Response
- Information Disposal
- IT Usage Authorization
- Information Handling
- Information Security Activity Review
- Violation Reporting
- Training and Awareness

Areas for which a more fully defined set of procedures is required will be noted and documented appropriately.

Security Management

Purpose

The objective of this policy is to implement guidelines and procedures to prevent, detect, contain, and correct security violations.

Risk Analysis

The University of Rhode Island has a responsibility to itself, its employees, and students to conduct a thorough assessment of potential risks and vulnerabilities both physically and technical. This analysis shall include a review of policies and procedures, physical security and technical security. An independent party not responsible for implementing or maintaining the systems being assessed may perform the assessment on an annual basis and a report will be delivered to The University of Rhode Island directors upon completion. Nothing in the timeframe for the assessment mentioned immediately above restricts the generation of periodic assessments, as will occasionally be required for operational and business reasons. Note: Periodic assessments need not be all encompassing of the entire organization. Periodic assessments can be defined to address the area of change only.

Application and Data Criticality Analysis

The University of Rhode Island maintains and accesses a variety of data, applications, and systems as part of its daily business. On an annual basis, University of Rhode Island Department managers and designated senior management staff will itemize and rate the importance of the applications, systems, and data that pertain to their departments and University as a whole. This rating will take into affect the implications a department would face if such items became unavailable. This data will be collected and processed by The University of Rhode Island CIO and Information Security Officer to determine the overall criticality of applications, data, and systems to The University of Rhode Island as a whole. The resulting analysis will be used to update the University's business continuity and disaster recovery plan.

Risk Management

The University of Rhode Island Information Security Officer has the responsibility of creating a list of deployed security measures physical, environmental, and technical. This list defines the purpose of the security measures and risk mitigated. As assessments are performed and new threats are realized, it is the Information Security Officer's responsibility to comment upon and recommend mitigation steps for the discovered threats or vulnerabilities.

Risk Acceptance Process

In rare circumstances, exceptions to information security policies and standards will be permitted if the Information Security Officer and the Department Manager have all signed a properly completed risk acceptance form. In the absence of such management approval reflected on a risk acceptance form, users must consistently observe relevant University of Rhode Island Information security policies and standards.

DRAFT

IT Usage Authorization

Purpose

This policy is intended to establish administrative measures to ensure that all members of The University of Rhode Island workforce has appropriate access to information, and to prevent those workforce members who do not have access from obtaining access.

Job Functions

All positions within The University of Rhode Island must have a clear job description and define the type of information access required in order to perform associated duties.

Granting of Data Access

Regardless of Job Function, an individual may not obtain access to data not classified as public until the following criteria have been met:

1. Individual has read and signed The University of Rhode Island Acceptable Usage / Privacy Policy
2. Individual has read and understood The University of Rhode Island:
 - **Information Security Policies**
3. Data owner has acknowledged in writing that the individual requires access to information.

Documentation of Data Access

The granting and removal of data access will be documented detailing name of individual, job function, data owner, type of access granted, date access granted or terminated.

On a semi-annual basis, data owners will review lists of individuals with data access and identify any inappropriate access.

Access Termination

Access termination may occur for a variety of reasons: job function changes, termination, extended leave are just some examples. Access Termination must come from the data owner; the individual's Department manager or the Human Resource Department. The purpose and date of access termination must be documented. Once access has been terminated, the individual terminating access must document compliance with the request.

Note: In the event access termination occurs due to involuntary employee termination. All data access should be terminated immediately. The individual in question should be escorted out of The University of Rhode Island facilities and all material should be examined to ensure non-public information is not contained within the belongings.

DRAFT

Data Backups and Recovery

Purpose

This policy is intended to provide guidance for the backup and recovery of data in its various forms, be it printed reports or electronic form. This policy is intended to address all information classification levels.

Responsibilities

The University of Rhode Island performs an electronic data backup on a daily basis of all critical servers. This backup is carried out by The University of Rhode Island Backup Administrator. It is the responsibility of all University of Rhode Island Employees to ensure all data is stored on central servers for backups. The University will not backup data which is stored on a departmental server, personal computer or other electronic device. Any such data will be the sole responsibility of the user assigned to the device.

Data Backups and Recovery

The backing up of Data is a critical step in securing University of Rhode Island Data and ensuring continued success. The loss of information would result in the loss of business and revenue for the University.

Electronic data will be encrypted and backed up on a regular basis. These backups will consist of full daily, full weekly and full monthly backups. Once a month, tests will be performed to ensure backup media is functioning properly. This test will encompass the recovery of data from the backup media. Furthermore, based upon information provided by backup software, the success or failure of backups will be noted daily and in the event of a failure; modifications will be made to ensure a successful future backup. These modifications will be recorded by the individual in charge of backups.

Printed reports and other forms of printed data will be stored within University of Rhode Island facilities within a locked safe.

Document/Data Retention

Monthly backup media will be archived for a period of (6) six years. Daily backup media will be reused (overwritten) on a two week cycle. Weekly backup media will be reused (overwritten) on a monthly cycle. Printed reports and other forms of printed data not slated for destruction will be stored for a period not to exceed (6) six years. As necessary, printed data may be recorded in a digitized formats (scanned, microfiche) and stored on electronic media. If such data contains sensitive information, it should be encrypted.

External Party Security

Purpose

This policy provides guidance for the handling and distribution of Restricted or Confidential data to Third-Parties. For the purpose of this policy the aforementioned information types will be referred to as **Sensitive Information**. Third-parties will be defined as non-University of Rhode Island employees.

While this policy describes the considerations one should bear in mind before, during, and after disclosure to third parties, it cannot specifically address every possible situation. Questions about disclosure should be directed to either a Department Manager or the relevant information owner.

Third Parties and the Need to Know

Unless it has specifically been designated as public, all sensitive information must be protected from unauthorized disclosure to third parties. Third parties may be given access to sensitive information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by the relevant information owner.

Non-Disclosure Agreements:

The disclosure of sensitive information to consultants, contractors, and temporaries must always be preceded by the receipt of a signed non-disclosure agreement (NDA). When a NDA pertains to an organization, to be valid, an Officer of the recipient organization must sign the NDA. Workers must not sign NDAs provided by third parties without the advance authorization of legal counsel designated to handle intellectual property matters.

Third Party Requests for Sensitive Information

Unless a worker has been authorized by management to make disclosures, all requests for information about the University and its business must be referred to the responsible data owner. Such requests include questionnaires, surveys, newspaper interviews, and the like. This policy does not apply to sales and marketing information about products and services, nor does it pertain to participant requests for information that have been approved for release to the participant.

Discussions in Public Forums

Care must be taken to properly structure comments and questions posted to electronic bulletin boards, electronic mailing lists, on-line news groups, and related forums on public networks like the Internet. If a user is working on an unannounced new service, a research & development project, or handling sensitive information, all related postings must be cleared with one's manager

prior to being posted to any public network. Likewise, workers should be careful not to reveal specifics about internal systems (such as configurations or products used) via public postings.

Disclaimers

It is the disclosing parties responsibility to make sure that when controversial, frequently changing, highly uncertain, or potentially-damaging information is released to third parties that it contain the appropriate legal disclaimers. Such disclaimers, generally provided by legal counsel, include words which limit liability, define the information's intended uses, and place recipients on notice of potential problems associated with the information.

Disclosure Records

Records reflecting that sensitive internal information (not information designated Public) has been distributed to third parties must be maintained by the worker releasing the information to the third party. Such records must indicate the types of information disclosed, the receiving third party's name and contact particulars (generally address, telephone number, and email address), as well as the date of release. Maintenance of such records will allow errors to be quickly corrected, allow updates to be quickly provided, allow recovery of the information, and also allow The University of Rhode Island to take legal action (should the third party use the information in unintended and unauthorized ways). It should be noted that even though a confidentiality agreement may have been signed, and even though management has approved third party access to certain information, it is still the responsibility of the worker releasing the information to keep records reflecting the information disclosed and to verify that the data is released to the proper intended recipient.

Reporting Improper Disclosures

If sensitive information has been inappropriately disclosed, or is believed to have been inappropriately disclosed, the circumstances must immediately be reported to the Information Security Officer. It is the responsibility of the Information Security Officer in conjunction with Legal Counsel and senior management to determine whether the disclosure or suspected disclosure needs to be reported to third parties such as criminal justice system personnel, participants, clients and others.

Information Security Activity Review

Purpose

In order to ensure the safety of information entrusted to The University of Rhode Island, access to data, systems, and supporting infrastructure must be monitored and reviewed. This policy provides for the establishment of monitoring and the review of system activity.

Responsible Parties

System Administrators are responsible for acting as information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They are also responsible for reporting all suspicious computer and information-security-related activities to the Information Security Officer. Administrators also serve as local information security liaisons, implementing the requirements of this and other information systems security policies, standards, guidelines, and procedures.

The Information Security Officer is responsible for the weekly collection and review of information-security-related activities. Based upon the results of the review, the Information Security Officer will make recommendations for improvements. The Information Security Officer is responsible for reporting a summary of activities to senior management.

Monitored Activities

At a minimum, The University of Rhode Island will monitor and log the following activities:

- Network Access (Example: Login and Logoff of users, Firewall activity, etc...)
- Application Access of application containing Restricted or Classified data.
- Network activity for security and performance
- Application history reporting showing user application activities.

Monitoring Periods

Where applicable and necessary, systems will issue security alerts to designated personnel. Designated personnel will respond to these alerts immediately. Log files will be monitored on a weekly basis for critical systems and on a monthly basis for non-critical systems.

Information Retention Period

Logged information will be maintained on appropriate systems for a period not to exceed one month. Information will then be archived in native system format onto read only electronic media and stored for period not to exceed 6 years.

Incident Handling and Response

Purpose

The objective of this policy is to provide guidelines and procedures to handle security violations once they have been reported.

Establishment of Incident Response Team and Responsibilities

To ensure a quick, effective, and orderly response to incidents, the individuals responsible for handling information systems security incidents must be clearly defined. These people are in turn responsible for defining procedures for handling incidents. Team members and responsibilities are:

- Chief Information Officer – Team Member. Authorized to expend funds as necessary to remedy incident.
- Information Security Officer – Team Leader. Centralized repository for collected data. Determines appropriate action to remedy incident. Maintains log of activity performed.
- IT Staff Representative – Team Member. Responsible for carrying out action as directed by Information Security Officer.
- Department Head of affected area – Team member. Responsible for informing related personnel of Teams decision and collecting information from related personnel to report to Incident Response Team
- Third-Party – Team Member. A qualified third-party should be brought in when necessary to aid in incident handling, forensics, and recovery.

Retention of Information Security Violation & Problem Information

Information describing all reported information security problems and violations must be retained for a period of six (6) years.

Annual Analysis of Information Security Violations & Problems

An annual analysis of reported information security problems and violations must be prepared by the Information Security Officer and be presented to The University of Rhode Island Senior Management.

Incident Response Testing

On a semi-annual basis, incident response team members will conduct response testing to ensure the effectiveness of the incident response procedures. This will be accomplished in a conference room question and answer session. The questions will propose possible incident scenarios and the appropriate team members will answer regarding actions to the incident.

Incident Handling Procedures

Incidents are defined as security violations. Security violations are a combination of alerts generated by software, security devices and technology, those detected through the analysis of the network traffic and log files generated software, and those suspected by University of Rhode Island personnel. Upon detection of suspicious activity, University of Rhode Island personnel will report such activity as detailed within the Violation Policy. The University of Rhode Island Security Incident Response Team will respond as detailed within the accompanying Security Incident Response Plan document.

Violation Reporting

Purpose

All suspected information security incidents must be reported as quickly as possible through the correct internal channels. If problems and violations go unreported, they may lead to much greater losses for the organization than would have been incurred, had the problems been reported right away. A good example of this involves computer viruses, which if unreported and uncontained, will continue to spread. Therefore, workers have a duty to report all information security violations and problems to the Information Security Officer or their Department Manager on a timely basis so that prompt remedial action may be taken.

Worker Protection

The University of Rhode Island will protect workers who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. This means that such workers will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation. Before taking any other action, these workers must report the problem to their manager or to Human Resources, and then give the organization time to remedy the situation.

Interference with Reporting Of Information Security Problems

Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action. Any form of retaliation against an individual reporting or investigating information security problems or violations is also prohibited and cause for disciplinary action.

External Reporting Of Information Security Violations

If required by law or regulation, management must promptly report information security violations to external authorities. If no such requirement exists, in conjunction with legal counsel, and the Information Security Officer, management must weigh the pros and cons of external disclosure before reporting these violations.

Reporting of Violations

Employees suspecting a violation must report said violation to their Information Security Officer or Department manager.

Information Disposal

Purpose

In order to insure the overall security of The University of Rhode Island data and to comply with various regulatory requirements regarding the destruction of data, this policy establishes guidelines for the proper disposal of information in its many forms that has been labeled as **Restricted or Classified** as defined by The University of Rhode Island Information Classification and Sensitivity Policy. For the purpose of this policy, these information types will be referred to as **Sensitive** data.

Electronic Data Disposal

Electronic data is constituted but not limited to data stored on a hard drive, digital tape, floppy disk, and recordings of voice conversations. Electronic media should be thoroughly cleansed of sensitive data prior to disposal or re-use. In the event of disposal, the media should undergo a degaussing step which results in the electronic media being rendered unusable, thereby resulting in the data being inaccessible. In the event of media re-use, be the media a computer hard drive, floppy disk, CD-Rom, etc..., the media must be cleansed of sensitive data. This may be accomplished through the use of multiple reformats of the data (3 times) or through the use of software designated by The University of Rhode Island for such purposes.

Physical Data Disposal

Physical data is constituted but not limited to printed reports, hand written notes, etc... Physical media must be physically destroyed to a point from which sensitive data cannot be recovered. For example, printed reports and hand written notes should be shredded when their usefulness is at an end.

Training and Awareness

Introduction

All workers (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect University of Rhode Island Information resources.

The specific material to be delivered to workers will vary based on the nature of the jobs that these workers perform. For example, administrative staff generally receives different training than the Information Technology staff. Nearly every worker accesses University of Rhode Island Information in order to do his or her job. Nonetheless, many workers need only rudimentary training. This policy relies on the Information Security Officer to decide what constitutes sufficient information security training. At a minimum, the training will constitute a review of The University of Rhode Island policies and procedures. Every worker must understand The University of Rhode Island policies and procedures about information security, and must agree in writing to perform his or her work according to such policies and procedures.

Training Time

It is not realistic to expect employees to read information security materials during their own time. Management must give their employees enough time to acquaint themselves with information security materials. Therefore, management must allocate sufficient on-the-job time for employees to acquaint themselves with The University of Rhode Island security policies, procedures, and related ways of doing business.

In addition, the Security Team will provide refresher courses and such other materials to regularly remind employees, temporaries, consultants, and contractors about their obligations with respect to information security.

Technical Information Systems Staff Training & Continuing Education

The University of Rhode Island management must allot sufficient funds and time for technical training and continuing education of the Information Systems staff. This prevents workers from being in a position where they could adversely affect business records (by errors, omissions, etc.) due to insufficient technical training.

Physical Safeguards

Introduction

This section of the policy manual addresses major areas of physically protecting information resources.

Areas addressed within this section include:

- Device and Media Controls
- Facility Security
- Computer/Network Security

Areas for which a more fully defined set of procedures is required will be noted and documented appropriately.

Device and Media Controls

PURPOSE

This document establishes operational standards for the handling of media and systems within The University of Rhode Island Information infrastructure.

SCOPE

This policy applies to all media containing University of Rhode Island Information and to all information systems (computers, servers, network devices, etc...)

Media Labeling

Based upon information classification, media (electronic or hard copy) shall be labeled as follows:

- ***Restricted:*** Electronic media containing restricted information should be labeled with the word “Restricted” in prominent view. Hard copies of such information should use a cover sheet with the word “Restricted” in prominent view, and where applicable, headers and footer of such reports should include the word “Restricted”.
- ***Classified:*** The majority of information within The University of Rhode Island is “Classified” as such; any unlabeled electronic media is assumed to contain confidential information and is to be treated as such. Hard copies such information do not require a label.
- ***Public:*** Electronic media containing Public information should be labeled with the words “Public” in prominent view.” Hard copies of such information should use headers and footers to include the word “Public”.

Media Reuse

In the event of media re-use, be the media a computer hard drive, floppy disk, CD-Rom, etc..., the media must be cleansed of non-Public data. This may be accomplished through the use of multiple reformats of the data (3 times) or through the use of software designated by The University of Rhode Island for such purposes.

Equipment Restrictions

Only computers purchased, leased or rented by The University of Rhode Island may be used for conducting the University business. Only the staff approved by the department is authorized to install and provide access to computers. All unauthorized installations are subject to removal.

Computer/Network Physical Security

PURPOSE

This document establishes operational standards for the physical security of University of Rhode Island data assets and systems.

SCOPE

This policy applies to all physical locations leased or owned by The University of Rhode Island. Throughout this policy, the word "facility" will be used to collectively refer to all such physical locations.

RESPONSIBILITIES

The Department Manager is responsible for ensuring employees are made aware of and adhere to this policy and that the security standards are followed within their respective departments.

Users are responsible for complying with this and all other University of Rhode Island policies defining computer and network security measures.

PHYSICAL SYSTEM SECURITY

Equipment Theft: To prevent theft, all office desktop computers (with the exception of portables) must be secured by a method approved by the Information Security Officer. All computer equipment is marked with identification information that clearly indicates it is The University of Rhode Island property. Periodic physical inventories are used to track the movement of Computers and related computer equipment.

Custodians for Equipment: The primary user of a Computer is considered a custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a custodian must promptly inform the involved department manager. Computer equipment must not be moved or relocated without the knowledge and approval of the involved department manager.

Use of Personal Equipment: Workers must not bring their own computers, computer peripherals, or computer software into University of Rhode Island facilities without prior authorization from the Information Technology department head.

Environmental Considerations

To reduce the damage done by electrical power problems, all Computers in The University of Rhode Island offices must use surge suppressers. Those Computers with critical production applications must also have uninterruptible power systems (UPSs).

If weather and/or building conditions pose a significant risk of static electricity discharge, Computers must be outfitted with static protection equipment that has been approved by The University of Rhode Island CIO. This will help prevent damage to equipment and the resident information. On a related note, magnetic storage media such as floppy disks and magnetic tapes must be kept at least several inches away from electric fields, such as those generated by a telephone when it rings.

PHYSICAL SECURITY OF COMPUTER AND COMMUNICATIONS GEAR

All University of Rhode Island network equipment must be physically secured if located in an open office environment that is assessable to non-employees. Local area network servers are placed within locked computer rooms.

Access to systems, development, staff offices, telephone wiring closets, computer machine rooms, and other work areas storing "non-public" information must be physically restricted.

Workers are prohibited from smoking, eating, or drinking when within The University of Rhode Island designated computer room.

Facility Controls

PURPOSE

To provide adequate building security for persons, property and data assets. This document establishes operational standards for the physical security of cubicles (where possible), offices, documents and personnel, physical assets and facility maintenance and modifications.

SCOPE

This policy applies to all physical locations leased or owned by The University of Rhode Island. Throughout this policy, the word "facility" will be used to collectively refer to all such physical locations.

RESPONSIBILITIES

The Department Manager is responsible for ensuring employees are made aware of and adhere to this policy and that the security standards are followed within their respective units.

Users are responsible for complying with this and all other University of Rhode Island policies defining computer and network security measures.

Visitor Guidelines

- The University of Rhode Island official business hours are Monday through Friday, 8:00 A.M. to 5:00 P.M. (except for official holidays).
- Within reason and practical limits, employees having visitors must escort them when within controlled areas.
- All other visitors (vendors, etc.) are required to report to a Reception area or Visitor Center where they are required to sign a visitor log book. They must receive and wear a visitor badge at all times.
- In order to ensure protection against sensitive information, employees may need to restrict others from entering their cubicle when such information is displayed, turn off their computer monitor or minimize the "window" they are working on. Employees are to ensure that sensitive material (in their possession) is locked up when not in use, and prior to departing their office for the day.
- Department heads should ensure sufficient illumination in and around facilities to allow the detection and observation of persons approaching the building and to discourage criminal activity.
- All employees need to be concerned with building lock-up and ensure that when entering and leaving the building after the normal business hours, the doors and office windows are locked. Employees are not to lend their building or office keys to anyone.

- Employees must share in the responsibility of questioning unescorted visitors and reporting any unauthorized personnel to The University of Rhode Island Information Security Officer.
- Visitors are not allowed access to the building without prior authorization.
- The CIO may issue special permission for individuals to be in the building without the escort of a staff member or display of a visitor badge. Such cases will be previously announced to staff.

PHYSICAL BUILDING SECURITY

Adequate building security is essential for the safety of employees as well as for The University of Rhode Island physical assets. Therefore the following physical security measures have been implemented within all facilities:

- All entrances to facilities will remain locked during non-business hours. Employees will be issued a key to the facility. A record will be maintained by the Information Security Officer (or designee) of key issuance detailing date of issuance and employee name. Should a key become lost, employee must notify the Information Security Officer within 2 hours. During such times that may result in the dismissal of a “disgruntled” employee, management must determine if new keys and locks are to be implemented.
- All facilities are equipped with ample smoke detection and fire detection and suppression.
- All facilities have detailed plans describing building exit strategies in the event of an emergency.
- All facilities are equipped with alarm systems design to detect intruders during non-business hours.

Clean Desk Requirements

The display screens for all Computers used to handle non-public or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas.

When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy non-public information must be locked in file cabinets, desks, safes, or other furniture. Likewise, when not being used, or when not in a clearly visible and attended area, all computer storage media (floppy disks, tapes, USB Drives, CD-ROMs, etc.) containing sensitive information must be locked in similar enclosures.

MAINTENANCE RECORDS

Over time various maintenance and modification to the building and office occur. During such times that these modifications affect the security of the facility, i.e. new alarm system, changing of locks, moving of computer room, these modifications will be documented and recorded. Such documentation will consist of:

- Type of modification
- Purpose of modification
- Name of Person(s) responsible for modification approval along with signature or other documentation granting approval.
- Dates of modifications (Start and End date)
- Name of Contractor or individual conducting the modifications
- If individual is not an employee of The University of Rhode Island, details of steps taken to limit individual's access to non-Public data.

Such records may be maintained in either printed or electronic form. Records will be maintained for (6) six years from the date of modification completion.

Technical Safeguards

Introduction

This section of the policy manual addresses key technical security controls and provides guidance and standards for using these controls.

Areas addressed within this section include:

- Audit Policy
- Encryption
- Software Development
- Transmission Security
- Access Controls

Areas for which a more fully defined set of procedures is required will be noted and documented appropriately.

Audit Policy

Purpose

This policy establishes guidelines for the recording and examination of activity on systems or networks that contain University of Rhode Island information.

Network Monitoring

The University of Rhode Island has deployed systems to record, detect, and issue alerts regarding intrusions from external and internal sources. These systems are comprised of network based intrusion detection systems and firewall logging. High level alerts are issued to the Information Security Officer for immediate review and response.

System/Application Monitoring

The University of Rhode Island has configured deployed systems to monitor system and application activity. Activity monitored includes:

- System/Application logons/logoffs
- Account management
- Files Access
- Data Access
- System Access

Activity is recorded to appropriate host/application log files.

Activity Review and Retention

The University of Rhode Island will review activity on a weekly basis. A summary report regarding incidents and activity will be provided to senior management on a monthly basis. Log files will be maintained on respective hosts and systems for 1 week and then archived for a period of 6 years.

Transmission Security

Purpose

Information is one of The University of Rhode Island most valuable assets. Its exposure could result in monetary or loss of reputation in the marketplace. This policy establishes guidelines to guard against unauthorized access to non-Public data being electronically transmitted over public and non-public (University of Rhode Island owned) networks.

Allowed Information Transmissions

University of Rhode Island workers may transmit information classified as “**Public**” to any recipient. Such information may be transmitted over public and non-public networks in a non-secure manner.

University of Rhode Island workers may transmit information classified as “**Classified**” or “**Restricted**” only to University of Rhode Island employees whose job function requires access to such data. This information may be transmitted across non-public networks unencrypted, however, “**Restricted**” data must be password protected prior to transmission. The transmission of these information classification types across public networks requires that the information be encrypted or the establishment of an encrypted link between University of Rhode Island non-public network and the recipient (i.e. VPN or an SSL tunnel).

Information Transmission Security

In order to secure the transmission of information within The University of Rhode Island non-public network, the network has been segmented into Virtual Local Area Networks (VLAN) that have been designed to group individual workers requiring access to like data into sub-networks. Access controls have been placed upon the VLANs to prevent access or unauthorized monitoring activity.

To secure the transmission of information not classified as “**Public**” across public networks, The University of Rhode Island is evaluating VPN connectivity with 2 factor authentication for remote access that will encrypt data during transmission. The University of Rhode Island will

deploy encryption technology to protect data transmitted to participants and third-parties that don't have access to The University of Rhode Island VPN.

DRAFT

Encryption

Purpose

This policy provides guidance in the use of encryption for the protection of information not classified as “**Public**” in its various electronic states.

Archived

The University of Rhode Island has deployed backup software which encrypts all data upon recording to archived media. This software requires the use of a password for data recovery and creates digital checksums in order to verify data integrity.

File Systems

The University of Rhode Island maintains information of various classification levels on shared files systems and within database applications. These file systems and applications are accessed by multiple individuals for a variety of reasons. Current encryption capabilities do not support The University of Rhode Island data sharing requirements, therefore, The University of Rhode Island has implemented a variety of monitoring and auditing techniques to validate the integrity and security of information not classified as “**Public**”. The techniques include history logs within applications, file access monitoring, file modification monitoring, and file deletion monitoring.

Across Networks

Refer to the policy “**Transmission Security**” for details regarding encryption use for information transmitted across networks.

Access Controls

Purpose

The policy provides guidelines dictating technical access controls for gaining access to The University of Rhode Island data. This policy is intended to address all information classifications levels except “Public”. For the purpose of this policy the aforementioned information types will be referred to as “Sensitive” information.

Scope

This policy applies to all workers (employees, consultants, contractors, temporaries, etc...). Where possible, access control requirements will apply to University of Rhode Island controlled information systems (applications, hosts (servers/workstations/network equipment), and the network) unless otherwise noted.

Unique Identifiers

The University of Rhode Island insists that each worker accessing multi-user information systems have a unique user-ID and a private password. These user-IDs must then be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each worker is personally responsible for the usage of his or her user-ID. User-IDs will be composed of first initial and surname. In the event of creation of an identical user-ID, additional letters from the first name will be used until a unique user-ID is created.

In those cases in which an information system does not support unique user-IDs (super user access (Administrator), single user environment, etc...), access to the user-ID will be restricted to a set of known University of Rhode Island employees. This set will be documented and upon the employment termination, the shared user-ID will modified if possible.

Authentication (Password Management)

To ensure that password systems do the job they were intended to do, users must choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. Each worker is personally responsible for the usage of his or her password.

Users can choose easily-remembered passwords that are at the same time difficult for unauthorized parties to guess if they:

- (a) String several words together (the resulting passwords are also known as "passphrases"),
- (b) Shift a word up, down, left or right one row on the keyboard,
- (c) Bump characters in a word a certain number of letters up or down the alphabet,
- (d) Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word,
- (e) Combine punctuation or numbers with a regular word,
- (f) Create acronyms from words in a song, a poem, or another known sequence of words,
- (g) Deliberately misspell a word (but not a common misspelling), or
- (h) Combine several preferences like hours of sleep desired and favorite colors.

To make guessing more difficult, passwords must also be at least eight characters long. To ensure that a compromised password is not misused on a long-term basis, passwords must also be changed every 30 days or at more frequent intervals, and cannot be used more than once a year. Whenever a worker suspects that a password has become known to another person, that password must immediately be changed. In addition, where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After five (5) unsuccessful attempts to enter a password, the involved user-ID must be either suspended until reset by a system administrator, or temporarily disabled for no less than thirty (30) minutes. If dial-up or other external network connections are involved, the session must be disconnected.

Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons might discover them.

If users need to share computer-resident data, they should use electronic mail, groupware databases, public directories on local area network servers, and other mechanisms. Although user-IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. To share a password (or for that matter any other access mechanism such as a dynamic password token) exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. If a worker believes that someone else is using his or her user-ID and password, the worker must immediately notify their Supervisor and the Information Security Officer.

Exceptions to sharing passwords to this involve:

1. Expired passwords, which are received at the time a user-ID is issued; these passwords must be changed the first time that the authorized user accesses the system.
2. Scenarios involving the sharing of a single user-ID. In those cases in which an information system does not support unique user-IDs (super user access (Administrator), single user environment, etc...), access to the user-ID will be restricted to a set of known University of Rhode Island employees. This set will be documented and upon the employment termination, the shared password will be modified and the user-ID will be modified if possible.

All other systems are to employ password protected screen savers that are provided with operating systems, so that after a period 15 minutes of no activity the screen will go blank until the correct password is again entered. Where possible, information system access throughout The University of Rhode Island will employ automatic log-out systems that automatically terminate a user's session after a defined period of inactivity, furthermore, where possible information systems will employ time access restrictions that prevent connectivity to the systems outside of defined work hours periods.

External Network Connectivity

All in-bound session connections to The University of Rhode Island internal networks from external networks (Internet, public dial-up lines, etc.) must be protected with an approved access control system. Users with personal computers connected to external networks are prohibited from leaving unattended modems turned-on while data communications software is enabled, unless an authorized password system has been previously installed. In general terms, workers

must not establish connections with external networks (including Internet Service Providers) unless these connections have been approved by the Information Security Officer.

Remote Access

Remote access is a management option, not a universal employee fringe benefit. Permission for remote access is granted by the involved employee's manager. The system privileges granted to all users, including remote access to University of Rhode Island systems, must be reevaluated by management every six months.

Workers must agree to and sign a Remote Access compliance form prior to being granted privileges to use dial-up, in-bound Internet access, or any other University of Rhode Island remote access data communications system.

Remote access to University of Rhode Island systems must occur over an encrypted link. Access must be restricted through the use of unique user-IDs and approved authentication methods. Employees using home computers for remote access must employ a personal firewall and up-to-date virus protection upon their home systems.

Employees granted remote access must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or access parameters that give access to University of Rhode Island systems with any other person.

Emergency Access

In the event of an emergency, system administrators may use emergency repair disks or other third party software to gain access to failed systems or other systems. In doing so, system administrators must document the systems in questions, types of failure, purpose of recovery, and data accessed.

Computer/Network Security

Purpose

The policy provides guidelines for the implementation of technical computer and network security measures.

Server Deployment

The University of Rhode Island has deployed multiple servers within its network environment. Each server is deployed to fulfill a specific purpose. Servers that are deployed should be using a standard, generic configuration check list. Further configuration is performed based upon the server's role. The role of the server, its further configuration changes, operating systems type, service pack level, and patch level are documented prior to installation upon the network. Any changes to the deployed servers are documented prior to placing the server back into production. Configurations are reviewed on a semi-annual basis to ensure documentation is correct.

Workstation Deployment

The University of Rhode Island has deployed workstations within its network environment for end-user usage. Each workstation should be deployed using a standard configuration check list detailing operating system, services packs, patch levels, and authorized software. Configuration modifications to individual workstations are documented.

Infrastructure Equipment Deployment

The University of Rhode Island has deployed a variety of Network Infrastructure equipment to include routers, switches, and firewalls. Configurations for these devices are maintained with semi-annual reviews performed to ensure documentation is correct and to address any configuration concerns.

Malicious Code Prevention (Virus, AdWare, Malware, Spyware, etc...)

In order to maintain the integrity, security and confidentiality of University of Rhode Island's information, The University of Rhode Island has deployed malicious code technology at the Internet gateway, servers, and workstations. Workstation and server software is configured to retrieve new malicious code signatures daily. The software monitors email and the file system. Gateway code prevention is provided by The University of Rhode Island's Perimeter Firewall and Managed Security Service Provider.