

# Implementing

IS-3

Electronic Information Security



University of California  
Office of the President  
Information Resources & Communications

September 7, 1999

# TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>1</b>
<b>PURPOSE</b>	<b>1</b>
<b>APPLICABILITY</b>	<b>1</b>
<b>RESPONSIBILITIES</b>	<b>2</b>
<b>ROLES</b>	<b>2</b>
<b>ELECTRONIC INFORMATION SECURITY GUIDELINES COORDINATOR</b>	<b>3</b>
<b>ELECTRONIC INFORMATION RESOURCE PROPRIETOR</b>	<b>5</b>
<b>ELECTRONIC INFORMATION RESOURCE CUSTODIAN</b>	<b>7</b>
<b>AUTHORIZED USER</b>	<b>8</b>
<b>FUNCTIONS</b>	<b>9</b>
<b>RISK ASSESSMENT</b>	<b>9</b>
<b>DISASTER RECOVERY</b>	<b>12</b>
<b>LOGICAL SECURITY</b>	<b>14</b>
<b>PHYSICAL SECURITY</b>	<b>19</b>
<b>MANAGERIAL SECURITY</b>	<b>20</b>

## INTRODUCTION

### **PURPOSE**

The purpose of these guidelines is to assist campuses in their implementation of Business and Finance Bulletin IS-3, Electronic Information Security.

- The guidelines list the tasks required by IS-3 according to the roles various members of the campus administration will play.
- The guidelines also summarize information about each of the security functions identified in IS-3.

These guidelines are only an introduction to Electronic Information Security. Business and Finance Bulletin IS-3 is rich in detail about the required electronic information security program.

### **APPLICABILITY**

Business and Finance Bulletin IS-3 applies to the security of Electronic Information Resources. These are data and resources:

- involving the *electronic* storage, processing or transmission of data, and
- used in support of the *administrative* business of the University.

Electronic Information Resources include: data (regardless of form); application systems, operating systems and tools, and communications systems; associated computer server, desktop, communications and other hardware.

## **RESPONSIBILITIES**

### ***ROLES***

The security of Electronic Information Resources is rarely the responsibility of a single individual or administrative unit. Those who play a role in the protection of Electronic Information Resources will work together in teams that cross functional units on the campus. Team members play one of four roles that have been identified in Business and Finance Bulletin IS-3. These are:

1. **Electronic Information Security Guidelines Coordinator** (the Coordinator). The person who has overall responsibility for coordinating campus compliance with Business and Finance Bulletin IS-3.
2. **Electronic Information Resource Proprietor** (the Proprietor). The individual to whom the Chancellor has delegated authority for an administrative function. By extension this is the department that determines the purpose and function of an Electronic Information Resource and controls access to it.
3. **Electronic Information Resource Custodian** (the Custodian). The individual or department that has physical or logical control over an Electronic Information Resource such as application systems or data processing equipment. Custodians may be staff in the department of the Proprietor, in central campus information technology or other departments, or in University or non-University enterprises with which the University has contracted.
4. **Authorized User** (the User). An individual who has been authorized by the Electronic Information Resource Proprietor to access an Electronic Information Resource. The authorization granted is for a specific level of access to a specific resource.

The responsibilities appropriate to each of these roles are identified in the next section.

## ***ELECTRONIC INFORMATION SECURITY GUIDELINES COORDINATOR***

The Coordinator identifies all individuals and units that are responsible for the security of campus Electronic Information Resources, provides education on the requirements of Business and Finance Bulletin IS-3, and ascertains that all required tasks have been completed. The Coordinator must:

1. Survey Proprietors and Custodians to identify all Electronic Information Resources designated as *essential*. (See Risk Assessment)
2. Survey Proprietors and Custodians to identify all Electronic Information Resources designated as *restricted*. (See Risk Assessment)
3. Ensure that disaster plans are prepared for *essential* Electronic Information Resources and coordinate their inclusion in the overall campus disaster recovery plan. (See Disaster Recovery)
4. Ensure that backup procedures have been implemented for *essential* Electronic Information Resources. (See Disaster Recovery)
5. Review logical controls on access to *essential* and *restricted* Electronic Information Resources. (See Logical Security)
6. Review logical controls (including change management procedures) on software associated with *essential* and *restricted* Electronic Information Resources. (See Logical Security)
7. Review logical controls (including adequacy of backup and retention) on data security for *essential* and *restricted* Electronic Information Resources. (See Logical Security)
8. Review logical controls on communications security for *essential* and *restricted* Electronic Information Resources. (See Logical Security)
9. Review logical protections against intrusive software for *essential* and *restricted* Electronic Information Resources. (See Logical Security)
10. Develop campus guidelines for the physical security of Electronic Information Resources. (See Physical Security)
11. Establish guidelines for determining which positions have job responsibilities that directly support *essential* Electronic Information Resources. (See Managerial Security)

12. Ensure that Proprietors or Custodians, as appropriate, conduct background checks on employees and consultants who have access to *essential* Electronic Information Resources. (See Managerial Security)
13. Ensure that Proprietors and Custodians, as appropriate, terminate access to *essential* Electronic Information Resources when employees and consultants change job duties or their affiliation with the University. (See Managerial Security)
14. Ensure that Proprietors and Custodians implement procedures to separate job duties, where appropriate, that directly support *essential* Electronic Information Resources. (See Managerial Security)
15. Designate a campus authority to track, take preventive measures against, and react to Intrusive Computer Software, such as computer viruses. (See Managerial Security)
16. Ensure that all security roles are filled for *essential* Electronic Information Resources. (See Managerial Security)

## ***ELECTRONIC INFORMATION RESOURCE PROPRIETOR***

The Proprietor is responsible for determining the level of security required based on the sensitivity and the level of criticality of an Electronic Information Resource. For those Electronic Information Resources deemed *essential*, the Proprietor determines the appropriate method of providing business continuity in case of disaster or emergencies. Proprietor also determines whether the Electronic Information Resource under its control is *restricted* and which users may have access to it. The Proprietor is responsible for specifying adequate data retention in accordance with University policies. The Proprietor must:

1. Identify all *essential* Electronic Information Resources in the control of the Proprietor. (See Risk Assessment)
2. Identify all *restricted* Electronic Information Resources in the control of the Proprietor. (See Risk Assessment)
3. Become familiar with the security requirements for *essential* Electronic Information Resources. (See Risk Assessment)
4. Ensure that Custodians prepare and test disaster recovery plans for *essential* Electronic Information Resources in the control of the Proprietor. This may require coordination with the Custodian and the Coordinator. (See Disaster Recovery)
5. Ensure that Custodians implement backup procedures for *essential* Electronic Information Resources in the control of the Proprietor. This may require coordination with the Custodian and the Coordinator. (See Disaster Recovery)
6. Grant access to Electronic Information Resources as required and consistent with guidelines set by the Coordinator. (See Logical Security)
7. Implement procedures for control of passwords for *essential* Electronic Information Resources. (See Logical Security)
8. Prepare guidelines for and control the use of shared passwords, if any, for *essential* Electronic Information Resources. (See Logical Security)
9. Revoke access to Electronic Information Resources as needed in response to violations of policy. (See Logical Security)

10. Ensure that the Custodian implements changes to *essential* and *restricted* software in accordance with University and campus systems development guidelines. (See Logical Security)
11. Implement the privacy requirements identified in UC policies. (See Logical Security)
12. Modify data in *essential* Electronic Information Resources software only in accordance with University and campus systems development guidelines. (See Logical Security)
13. Notify Authorized Users not to transfer or download *essential* or *restricted* data from secure to non-secure environments. (See Logical Security)
14. Ensure conformance to campus guidelines for the physical security of Electronic Information Resources in the control of the department. (See Physical Security)
15. Identify positions having job responsibilities that directly support *essential* Electronic Information Resources in the control of the department. (See Managerial Security)
16. Perform background checks on employees and consultants who have job responsibilities that directly support *essential* Electronic Information Resources. (See Managerial Security)
17. Implement procedures to terminate access to *essential* Electronic Information Resources, as appropriate, when employees and contractors change job duties or their affiliation with the University. (See Managerial Security)
18. Ensure appropriate separation of job duties, where appropriate, for positions that directly support *restricted* and *essential* Electronic Information Resources. (See Managerial Security)

## ***ELECTRONIC INFORMATION RESOURCE CUSTODIAN***

The Custodian is responsible for implementing security measures in accordance with the level of security required by the Proprietor.

1. Become familiar with the security requirements for *essential* Electronic Information Resources. (See Risk Assessment)
2. Prepare and test disaster recovery plans for *essential* Electronic Information Resources under the control of the department. This may require coordination with the Proprietor and the Coordinator. (See Disaster Recovery)
3. Implement backup procedures for *essential* Electronic Information Resources under the control of the department. This may require coordination with Proprietor and the Coordinator. (See Disaster Recovery)
4. Maintain systems logs, where feasible and appropriate, to monitor access to *restricted* and *essential* Electronic Information Resources. (See Logical Security)
5. Treat system logs that record access activity according to the privacy requirements identified in UC policies. (See Logical Security)
6. Back up Electronic Information Resources according to the level of security required and in conformance with University records retention guidelines. (See Logical Security)
7. Install firewalls to limit unauthorized access to *restricted* and *essential* Electronic Information Resources. (See Logical Security)
8. Use encryption, where feasible, to prevent unauthorized access to *restricted* data during transmission. (See Logical Security)
9. Implement procedures, commensurate with risk, to detect viruses, warn users, and take remedial action after a software intrusion. (See Logical Security)
10. Implement campus guidelines for the physical security of Electronic Information Resources. (See Physical Security)
11. Test software used to provide access controls and access control points for connectivity. (See Managerial Security)
12. Ensure periodic, independent review of superuser logs. (See Managerial Security)

## **AUTHORIZED USER**

Authorized Users of Electronic Information Resources are responsible for familiarizing themselves with and complying with all University policies, procedures and standards relating to information security. Authorized Users are responsible for appropriate handling of Electronic Information Resources as established and implemented by the Proprietors and Custodians.

1. Observe guidelines regarding the use of passwords and other mechanisms intended to protect Electronic Information Resources from unauthorized access. (See Logical Security)
2. Use *essential* or *restricted* data only for approved purposes and observe the privacy requirements in University policies. (See Logical Security)
3. Do not transfer *essential* or *restricted* Electronic Information Resources from secure to non-secure equipment or store them in areas that do not have controls on physical access. (See Logical Security)
4. Report violations of IS-3 guidelines to the appropriate campus authority. (See Managerial Security)

## FUNCTIONS

### **RISK ASSESSMENT**

See IS-3, Section IV, Risk, Sensitivity, and Criticality

### **Security Requirements**

Each campus must determine which specific Electronic Information Resources require security measures based on a risk assessment.

When determining the level of security required for an Electronic Information Resource, there are two basic risk characteristics to be assessed: *sensitivity* and *criticality*

The *sensitivity* of the Electronic Information Resource determines the level of access controls required.

The *criticality* of the Electronic Information Resource determines whether it must be included in Disaster Recovery Plans as part of overall business continuity planning.

		<b>Electronic Information Resource Criticality</b>		
		<b>Essential</b>	<b>Required</b>	<b>Deferrable</b>
<b>Data Sensitivity</b>	<b>Restricted</b>	<ul style="list-style-type: none"> <li>• Requires access security</li> <li>• Must be in Disaster Recovery plan</li> </ul>	<ul style="list-style-type: none"> <li>• Requires access security</li> <li>• May be in Disaster Recovery plan</li> </ul>	<ul style="list-style-type: none"> <li>• Requires access security</li> <li>• Need not be in Disaster Recovery plan</li> </ul>
	<b>Unrestricted</b>	<ul style="list-style-type: none"> <li>• Minimal security required</li> <li>• Must be in Disaster Recovery plan</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal security required</li> <li>• May be in Disaster Recovery plan</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal security required</li> <li>• Need not be in Disaster Recovery plan</li> </ul>

**Sensitivity**

The Proprietor is responsible for determining the level of security needed, based on the sensitivity of the data retained by or accessible through the Electronic Information Resource.

The same data may be classified differently for different purposes. For example, it may be *unrestricted* for read-only access but *restricted* for modification.

The Electronic Information Resource is *restricted* if its data is considered sensitive for either read-only access or for modification access.

*Restricted* Electronic Information Resources require access security.

Sensitivity Checklist	Yes	No
1. Does the data include information that identifies or describes an individual?		
2. Would unauthorized access, modification or loss of the data seriously affect the University?		
3. Would unauthorized access, modification or loss of the data seriously affect a business partner of the University?		
4. Would unauthorized access, modification or loss of the data seriously affect the public?		
5. Has the Proprietor chosen to protect the data from general access or modification?		

If the answer to all these questions is No, the data is *unrestricted*.  
 If the answer to any of these questions is Yes, the data is *restricted*.  
 If the answer to question 1 is Yes, the data is *personal* (a subcategory of *restricted*).  
 If the answer to either question 2, 3, 4, or 5 is Yes, the data is *limited* (a subcategory of *restricted*).

**Criticality**

The Proprietor is responsible for determining the level of criticality of an Electronic Information Resource.

Criticality is a measure of the importance of an Electronic Information Resource to the continuing operation of a campus.

The designations *essential*, *required*, or *deferrable* may be applied to various types of Electronic Information Resources (software and hardware).

The same Electronic Information Resources may be designated *essential*, *required*, or *deferrable* under different circumstances, depending on the period of inoperability.

Campuses must include all *essential* Electronic Information Resources in a campus Disaster Recovery Plan.

Criticality Checklist	Yes	No
1. Does the Payroll/Personnel system (PPS) directly depend upon the resource for on-going successful operation?		
2. Does the campus data network directly depend upon the resource for on-going successful operation?		
3. Does the campus telephone system directly depend upon the resource for on-going successful operation?		
4. Does the campus public safety communications system directly depend upon the resource for on-going successful operation?		
5. Will the campus be unable to perform an important administrative function correctly and on schedule if the resource fails?		
6. Will the campus sustain a significant loss of funds if the resource fails to function correctly and on schedule?		
7. Will the campus sustain a significant liability or other legal exposure if the resource fails to function correctly and on schedule?		
8. Will the campus be able to continue operation for a designated period of time if the resource fails to function correctly and on schedule?		
9. Will the campus be able to continue operation for an extended period of time if the resource fails to function correctly and on schedule?		

If the answer to *any* of questions 1-7 is Yes, the resource is *essential*.

If the answer to questions 1-7 is No and the answer to question 8 is Yes, the resource is *required*.

If the answer to questions 1-7 is No and the answer to question 9 is Yes, the resource is *deferrable*.

## **DISASTER RECOVERY**

See IS-3, Section V, Disaster Recovery and Emergency Procedures

Proprietors are responsible for ensuring that disaster recovery plans are prepared for *essential* Electronic Information Resources under their control.

The campus Coordinator should ensure that disaster recovery plans for *essential* Electronic Information Resources are coordinated with the overall campus Disaster Recovery Plan.

Disaster recovery plans are optional for *required* and *deferrable* Electronic Information Resources.

### **Disaster Recovery Planning Process**

1. Create a disaster recovery plan for *essential* Electronic Information Resources.
2. Update the disaster recovery plan periodically.
3. Test the disaster recovery plan regularly.
4. Coordinate plans for *essential* Electronic Information Resources with the overall campus Disaster Recovery Plan.
5. Include disaster recovery requirements in vendor agreements that pertain to *essential* Electronic Information Resources.

### **Disaster Recovery Plan**

1. Provide for running *essential* applications at alternative sites or by alternate means of processing.
2. Specify emergency response procedures.
3. Include requirements and procedures for offsite backup.

### **Emergency Procedures**

1. Assign personnel to implement emergency procedures.
2. Identify ways for personnel to contact each other during emergencies.

### **Backup Procedures**

1. Store backup copies of *essential* resources (data and software) in a commercial or equivalent offsite facility.
2. Verify that the backup facility provides adequate protection against fire, flood, earthquake, theft, decay, and other hazards.

## **LOGICAL SECURITY**

See IS-3, Section VI, Logical Security

### **Access Controls**

The Coordinator is responsible for review and approval of the means used to provide the security for *restricted* and *essential* Electronic Information Resources.

The Proprietor determines which Authorized Users may access an Electronic Information Resource and the level of access that will be permitted.

Access to *restricted* Electronic Information Resources must be limited to *Authorized Users*.

### **Access Procedures**

1. Incorporate review and approval mechanisms as part of the procedures that initially provide users with authorization for access to *restricted* or *essential* Electronic Information Resources in order to avoid unauthorized persons being granted access.
2. Require that requests for authorization to access to *restricted* or *essential* Electronic Information Resources and assignment of the level of access privilege be reviewed by the Proprietor.
3. Implement techniques for performing authentication and authorization before a user is granted access to *restricted* or *essential* Electronic Information Resources.
4. Retain authorization records consistent with University Records retention guidelines.

### **Violations of IS-3**

1. Do not attempt to gain unauthorized access to any Electronic Information Resources or to damage, alter, or disrupt their operation in any way.
2. Do not capture, obtain, or tamper with passwords, encryption keys, or any other access control mechanism that could permit unauthorized access (except where expressly required in the performance of one's duties).

3. Withdraw the privileges of any Authorized User who violates IS-3 when continuation of privileges threatens the security of a *restricted* or *essential* Electronic Information Resource.
4. Follow normal campus conflict resolution procedures for appeals regarding revocation of privileges.

### Passwords

1. Establish procedures that make passwords hard to guess and, for *essential* Electronic Information Resources, require them to be changed frequently.
2. Prohibit shared passwords for access to data that is *essential* or *restricted*.
3. Permit shared passwords only when:
  - the access is limited to a specific Electronic Information Resource,
  - sharing is essential to the continuity of an authorized business practice associated with that Electronic Information Resource, and
  - all other Authorized Users are authorized to at least the same level of access privilege.
4. Establish specific accounts for that purpose when there is a need for shared passwords.

### Modification of *Essential* Data

1. Modify *essential* data according to procedures established to ensure data integrity, availability, privacy, and compliance with audit requirements.
2. Do not circumvent data integrity and audit controls.
3. Make exceptions, if needed, only on a case-by-case basis, in a controlled manner, and with the knowledge of the Proprietor.

### Access Logs

1. Use system logs, where feasible and appropriate, to monitor access to Electronic Information Resources.

2. Include enough detail in system logs to ensure that suspicious patterns of activity can be identified.
3. Protect personally identifiable information in systems logs.
4. Consider use of system tools for automatic identification of suspicious patterns of activity within the logs.

### Overprotection

Do not protect Electronic Information Resources to the extent that Authorized Users cannot access them.

## Access Controls For System Administration

### Superuser Accounts

1. Limit superuser accounts to personnel whose job duties require them.
2. Provide superusers with less powerful accounts to use when not performing system administration tasks.
3. Instruct superusers not to use superuser accounts for other than authorized purposes.
4. Log activities performed using a superuser account.
5. Provide regular, independent review of superuser access logs to ensure they are being used for designated purposes.
6. Print or store superuser access logs in a non-subvertible form, where feasible.

## Software Control

For development and maintenance of administrative applications that are *essential* or *restricted*:

1. Conform to the specifications of BFB IS-10, Systems Development Standards, as well as to campus standards, procedures, guidelines and conventions.
2. Invite Internal Audit and the campus Controller to participate early in the design process in order to obtain advice on establishing proper controls.
3. Use only authorized personnel and use change management procedures established by the campus when revising software.
4. Assign responsibilities so as to ensure adequate separation of duties.

## Data Security

1. Make sure backup copies of data and software associated with *restricted* and *essential* Electronic Information Resources meet:
  - Disaster Recovery requirements
  - Application or other Electronic Information Resource processing requirements
  - Functional requirements of the department dependent upon such data.
2. Store backup copies of *essential* data at a commercial or an off-campus site that provides standard protection for Disaster Recovery purposes
3. Backup *restricted* and *essential* software and data stored on personal computers as well as software and data stored on shared servers.
4. Comply with University of California policies regarding data retention.
5. Conform to University policies and regulations related to privacy of data or information records associated with them.
6. Ensure that, when *essential* or *restricted* data is transferred from one server to another or to a workstation, access controls on the destination system are commensurate with:
  - access controls on the originating server and
  - the security requirements established by the Proprietor.

### Communications Security

1. Use firewalls to limit unauthorized access to *restricted* and *essential* Electronic Information Resource across campus or University communication networks
2. Encrypt *restricted* data during transmission, where feasible and appropriate, to prevent unauthorized access.
3. Consider use of intrusion detection systems to help identify attempted or actual unauthorized intrusions.

### Intrusive Software

1. Evaluate exposure to adverse intrusive computer software for different Electronic Information Resources.
2. Put protections in place commensurate with the level of risk and the associated cost to the institution for such anticipated loss.
3. Implement processes to notify users and take other appropriate remedial action in the event of propagation of Intrusive Computer Software.

## **PHYSICAL SECURITY**

See IS-3, Section VII, Physical Security

The campus Coordinator develops policies and procedures for the physical security of campus Electronic Information Resources that are *restricted* or *essential*.

Proprietors and Custodians implement procedures for the physical protection of Electronic Information Resources housed within their immediate work area, especially personal computers and other portable resources.

Proprietors maintain inventories of equipment in accordance with BFB Bus-29, Management and Control of University Equipment.

Authorized Users protect *restricted* data by not storing it on separate portable equipment such as laptops.

### **Disaster & Emergency Functions**

- Prevention
- Early Warning
- Detection
- Recovery

### **Physical Security Checklist**

1. **Disaster and Emergency Conditions** - Protect *restricted* or *essential* Electronic Information Resources from earthquake, fire, water leakage or flooding, disruption of power, air conditioning failures, and environmental conditions exceeding equipment limits.
2. **Physical Access** - Protect facilities housing *restricted* or *essential* Electronic Information Resources through the use of combination locks, key locks, badge readers, sign in/out logs for visitors, verification of identification, etc.
3. **Theft, Damage and Improper Use** - Protect all of the following *restricted* or *essential* Electronic Information Resources:
  - physical equipment,
  - software and data residing on storage media,
  - check stock, produced checks, and other financial instruments.

## **MANAGERIAL SECURITY**

See IS-3, Section VIII, Managerial Security

Proprietors are responsible for controlling access to *restricted* or *essential* Electronic Information Resources under their control.

Supervisors must inform the Proprietor of an individual's job duties: when access to *restricted* or *essential* Electronic Information Resources is requested, when those job duties change, and when if the individual's affiliation with the University changes.

### **Personnel**

Note - All procedures must be established in accordance with University personnel policies and guidelines. See Personnel Policies for UC Staff Members.

#### **For All Staff Positions**

1. Notify the Proprietor of any significant changes in job duties or other status if these changes require modification to the Authorized User's access authorization.
2. Remove access authorization for Authorized Users who have terminated employment or other association with the University (except where specifically permitted by Policy and by the Proprietor).
3. Remove access authorization for Authorized Users who have announced their decision to terminate if continued access might result in an unacceptable level of risk.
4. Ensure appropriate separation of duties when assigning job responsibilities that directly support *restricted* or *essential* Electronic Information Resources. (For example, no one individual should have authorization for both putting programs into production and updating production data.)
5. Periodically review the system administration work of personnel with access to privileged "superuser" accounts on shared servers. (Such review is intended to provide a periodic audit or review for those system administration functions that are not otherwise audited or reviewed in the course of being completed.)

**For Staff in Critical Positions**

For *restricted* or *essential* Electronic Information Resources:

1. Conduct applicable background checks as part of the hiring process.
2. Establish procedures that can be implemented in the event of disciplinary action or termination.
3. Restrict, suspend or terminate access where there is a concern that access to an Electronic Information Resource endangers the integrity of the resource.
4. Revoke access to the work location, if warranted, during an investigatory leave or after termination.

**For Contractors and Consultants**

For *restricted* or *essential* Electronic Information Resources:

1. Conduct background checks on non-University contractors or consultants.
2. Limit outside vendor access.
3. Revoke outside vendor access when the work has been completed.

**Escalation Procedures**

1. Authorized Users report any violation of IS-3 to the Proprietor, the Custodian, or the Internal Audit department.
2. The Proprietor or the Custodian takes prompt action to protect against future violations to the extent feasible, and/or remove the means by which the violation of IS-3 occurred.
3. The Proprietor or the Custodian consults with other campus authorities in accordance with policies governing potential disciplinary action for violation of IS-3.
4. The Proprietor or the Custodian notifies Internal Audit or the Police (in accordance with Business and Finance Bulletin G29, Procedures for Investigating Misuse of University Resources) if the violation of IS-3 involves possible unlawful action by a Authorized User.

Notification of Internal Audit or the Police should take place before any action is taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policy, or significant liability to the University or to members of the University community.

5. The University reserves the right to revoke access to any Electronic Information Resource for any Authorized User who violates IS-3, or for any other business reasons in conformance with other applicable University or campus policies.

### Testing

The Coordinator reviews logical controls on communications security for *essential* and *restricted* Electronic Information Resources, including procedures for testing software used to provide logical access controls and access control points for connectivity (e.g., firewalls).

### Intrusive Software

The Coordinator designates a campus authority to coordinate tracking, taking preventive measures, and reacting to Intrusive Computer Software such as computer viruses.