**Borrowed and adapted from a model created by University of Virginia**

### IT Security Risk Management Process Flow

w_bnidno[1]w_bnidno[1]w_bnidno[1]

1. **Disaster recovery plan example**
2. **Interim manual procedures example**
3. **Criteria**
4. **Template**
5. **Assessment questions**
6. **Threat scenarios**
7. **Response strategies**
8. **Security plan template & example**

*Security*

*Plan*

*Interim*

*Manual*

*Procedures*

*Disaster*

*Recovery*

*Plan*

Step 4 – Evaluation and Reassessment

Required at least once every two or three years

Step 3 – Mission

Continuity Planning

Create a response plan to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed

Step 2 – Assess Risks

For each critical asset:

1. Assign weight to likelihood & impact of threats to each asset
2. Prioritize threats
3. Select response strategies
4. Develop security plan

*Critical*

*Assets*

*List*

Step 1 - Identify

Critical IT Assets

## Step 2: IT Risk Assessment

In Step 1 you identified the critical IT assets in your department. In Step 2 you will analyze the risks facing those assets and identify and prioritize strategies for protecting them.

A focus on departmental mission is vital; departments cannot – and are not expected to – mitigate every risk but must prioritize based on the threat to their mission and available resources.

Three sets of templates and/or tools are included to assist in this process:

*2.1* ***Risk assessment questions*** *(with paths determined by applicability of laws)*

* Assess departmental security practices against University, national and international standards

*2.2* ***Threat, attack and vulnerability scenarios*** *(with response strategies)*

* Map your department’s assets from Step 1 to the threat scenarios provided (and others that your department identifies)
* Assign weight to each threat to your assets based on the likelihood of it occurring in your environment and the impact of any vulnerability
* Prioritize the threats you face
* Map these threats back to response strategies provided (and others your department develops)

*2.3* ***Security plan development*** *(template)*

* Create (or update if you already have one) your department’s security plan for mitigating or accepting the identified risks
* Take into account previously implemented strategies and existing plans – use (and document) effort and analysis that you have already produced
* Document your key decisions and justifications

### Step 2.1: Risk Assessment Questions

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Risk Assessment Questions: General  These questions will help determine and evaluate threats to the resources identified through a mission impact analysis, as well as adherence to general secure computing practices. | | | |
|  | Yes | No | Documentation location or explanation for not following |
| ***A. Physical Security*** | | | |
| 1. Are all computers located in areas that are not easily accessible to outsiders? |  |  |  |
| 2. Are mission critical systems located in a locked location to which access is restricted to authorized personnel only? |  |  |  |
| 3. Are faculty and staff taking responsibility for locking doors and windows where computers are housed? |  |  |  |
| 4. Has physical security been reviewed with the University Police and Facilities Management? |  |  |  |
| 5. Are department desktops and notebooks equipped with anti-theft devices? |  |  |  |
| 6. Are departmental keys logged in and out individually with one staff person responsible for the tracking of the keys? Has this procedure been approved by Facilities Management (FM)? |  |  |  |
| 7. Are department servers physically secure in a separate area, i.e., physically restricted, a double-locked door, with card access and access logging.? |  |  |  |
| 8. Are servers in environmental control areas that include:  Smoke detectors?  Water detectors?  Fire suppression systems?  Temperature sensors? |  |  |  |

|  | Yes | No | Documentation location or explanation for not following |
| --- | --- | --- | --- |
| 9. Are mission critical servers away from high-traffic areas; e.g., not near an auditorium or along a well-travelled hallway? |  |  |  |
| 10. Are uninterruptible power supplies (UPS) with surge protection used on servers and other important hardware? |  |  |  |
| 11. Are surge protectors (at least) used on desktop computers? |  |  |  |
| 12. Are individual firewalls (software or hardware) installed on any desktops, laptops or servers in the department? |  |  |  |
| 13. Are security incidents (for example, unauthorized use, loss, theft, or compromise of devices) reported in compliance with the IT Security Incident Reporting policy? |  |  |  |
| 14. Is there an accurate inventory of all computing equipment and software? If so, is a copy of the inventory stored off-site? |  |  |  |
| 15. Do you have individual use devices with sensitive data in a publicly accessible area? |  |  |  |
| ***B. Account & Password Management*** | | | |
| 1. Do you have defined, documented criteria for granting access based on job responsibilities? |  |  |  |
| 2. Are all sensitive data used for authenticating a user, such as passwords, stored in protected files? |  |  |  |
| 3. Are users authorized to access only those resources required to perform their jobs and nothing more? |  |  |  |
| 4. Does the department deactivate accounts for terminated or transferred employees in a timely manner? |  |  |  |
| 5. Does the department periodically review current employee accounts that have not been used in a long time and consider deactivating them? |  |  |  |
| 6. Does the department prohibit shared accounts? If shared accounts are not prohibited, please list what systems/applications require shared accounts and justify continued use. |  |  |  |
| 7. Has the department emphasized to users that their password, along with their computing ID, is the key to their electronic identity? |  |  |  |
| 8. Does the department have a policy on keeping passwords confidential? |  |  |  |
| 9. Does the department assist users in selecting passwords that will ensure privacy while promoting regular use? |  |  |  |
| 10. Does the department require that passwords not be written down or shared, except for purposes of escrow? |  |  |  |
| 11. Does the department securely escrow passwords for accounts that may need to be accessed in the absence of their normal administrator or in an emergency situation? |  |  |  |
| 12. Does the department require that passwords on departmental workstations and servers be changed periodically? |  |  |  |
| 13. Is there a reasonable “previous used” password history list to deter users from repetitive use of the same password? |  |  |  |
| 14. Does the department require passwords for access to department workstations and servers? |  |  |  |
| 15. Does the department require the use of password-protected screen savers, automatic application timeouts and automatic network log-offs? |  |  |  |
| 16. Does the department log and review more than three attempts to enter a password for a given account? |  |  |  |
| 17. Does the department prohibit modems attached to servers and desktops that can receive calls? |  |  |  |
| C. Virus Protection | | | |
| 1. Is anti-virus software installed on all department computers? |  |  |  |
| 2. Is a procedure for updating the anti-virus software in place? For personal systems, if this is up to the user, are instructions and recommended update intervals provided? |  |  |  |
| 3. Does the department periodically remind users to open only attachments they are expecting? |  |  |  |
| ***D. Data Backup and Recovery*** | | | |
| 1. Have faculty and staff been advised of their personal computer backup options? Do they have instructions for the options and recommended backup cycles? |  |  |  |
| 2. Does the department regularly back up department servers? Does the server backup procedure include secure off-site storage? |  |  |  |
| 3. Does the department periodically test restoration of personal and server files? |  |  |  |
| 4. Do users store all local data in a single directory to simplify backup of personal data and ensure all data is captured? |  |  |  |
| 5. Are backup needs periodically reviewed? |  |  |  |
| 6. Does the department comply with University’s Records Retention and Disposition Policy? |  |  |  |
| 7. Does the department consult with the University Records Officer before implementing any electronic document management system? |  |  |  |
| E. Operating Systems | | | |
| 1. Are only officially allowed operating systems used? |  |  |  |
| 2. Are appropriate operating system updates and security patches being applied in a timely manner to all department computers and servers? |  |  |  |
| 3. Are servers and desktops periodically scanned by IT services for security vulnerabilities? |  |  |  |
| 4. Have unnecessary services and features in desktop and server operating system configurations been disabled? |  |  |  |
| 5. Is the use of shared drives or folders between desktop computers (peer-to-peer sharing) prohibited or restricted? |  |  |  |
| 6. Is it verified that file permissions are properly set on servers? |  |  |  |
| 7. Is Autorun and AutoPlay functionality disabled for removable disks and shares? |  |  |  |
| F. Application Software | | | |
| 1. Are appropriate application software updates and security patches being applied in a timely manner to electronic devices *on which University-related data reside or business is done* (whether University or personally owned devices)? |  |  |  |
| 3. If employees are allowed to install University applications at home, is it installed in compliance with the license, with security of the device, and has any necessary user acceptance form been completed and returned to the appropriate person? |  |  |  |
| 4. Does the staff have the appropriate level of access to applications based on their current responsibilities? |  |  |  |
| 5. Is application access promptly removed for employees who have left the department? |  |  |  |
| G. Confidentiality of Sensitive Data | | | |
| 1. Are all departmental locations of highly sensitive data, both electronic and paper, inventoried? |  |  |  |
| 2, Following the Electronic Data Removal policy,   1. are all data and software removed from hardware and electronic media prior to transfer within the university 2. are all hardware and media processed through appropriate Security check, Property Disposal, Transporting to the Depot, etc. when leaving the university? Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices. |  |  |  |
| 3. Is access to sensitive departmental data restricted? |  |  |  |
| 4. Is ownership of data clearly defined? |  |  |  |
| 5. Do data owners determine and periodically review appropriate levels of data security required? |  |  |  |
| 6. Is access to information technology resources explicitly granted to personnel by data owners? |  |  |  |
| 7. Have the faculty who are conducting research determined if the data they are collecting should be classified as sensitive? |  |  |  |
| 8. Do the faculty and staff who administer sensitive data understand and follow appropriate federal, state, grant agency, or university regulations for protecting and backing up data? |  |  |  |
| 9. Are student workers given access to confidential teaching, research or administrative data? If so, is their use of such data monitored closely? |  |  |  |
| 10. Are authentication, authorization, and data security policies established by data owners protected from compromise during data sharing and systems interoperability? |  |  |  |
| 11. Are user agreements clearly stating required authentication and protection levels established with all external agencies and institutions with which data are shared?  List all such data sharing relationships, indicating the data shared and the transmission method used (e.g. VPN, SFTP). |  |  |  |
| 12. Is the unencrypted transmission of highly sensitive data through e-mail prohibited? |  |  |  |
| 13. Do web-enabled transactions that require user authentication, transfer highly sensitive data, or transfer funds use encryption? |  |  |  |
| 14. Are the employees who have VPN access aware they should be disconnecting from the VPN when not in use and when away from their desk? |  |  |  |
| 15. If the department has a wireless network, is the network encrypted? If so, what type of encryption? |  |  |  |
| 16. Are cryptology technologies for data storage and transmission of data based upon open standards? |  |  |  |
| 17. Are encryption key management policy and procedures in place to ensure the integrity and recovery of encryption keys? |  |  |  |
| 18. Are all sensitive data stored and transmitted in compliance with the University’s Institutional Data Protection Standards and the Electronic Storage of Highly Sensitive Data policy? |  |  |  |
| 19. Do all iKey hardware token users disconnect from the VPN when not in use and/or when away from their desk? Are users aware of their responsibilities regarding the protection of the iKey token? |  |  |  |
| 20. Are all highly sensitive data files routinely and promptly deleted in a secure manner when no longer needed for their approved business purpose or official records retention? |  |  |  |
| 21. If highly sensitive data are stored on individual use devices or media, has the appropriate vice president or dean completed the approval form? |  |  |  |
| 22. If highly sensitive data are stored on individual use devices or media, is it encrypted? |  |  |  |
| 23. If highly sensitive data are stored on individual use devices or media, are all security requirements strictly followed? |  |  |  |
| 24. Do you have a regular schedule for scanning departmental devices for highly sensitive data? If so, what is it? |  |  |  |
| 26. Have you returned your SSN Inventory and Remediation Status Report, indicating that you have completed your remediation plan? |  |  |  |
| H. Security Awareness and Education | | | |
| 1. Are faculty and staff aware of their responsibility for computer security according to the University Policy? |  |  |  |
| 2. Have all copies of department software been properly licensed and registered? |  |  |  |
| 3. Has the University’s copyright policy been distributed and discussed within the department? |  |  |  |
| 4. Have University and department-specific security policies and procedures been documented and shared with all faculty and staff? |  |  |  |
| 5. Are faculty and staff keeping current on faculty and university security issues and alerts? |  |  |  |
| 6. Are suspected violations of security appropriately reported to a designated system or departmental administrator? |  |  |  |
| 7. Do your system administrators and other IT managers have training commensurate with the level of expertise required, which may include ability to identify threats, vulnerabilities and risks specific to your information resources? |  |  |  |
| 8. Are individuals involved in information technology management, administration, design, development, implementation, and/or maintenance aware of their security responsibilities and how to fulfill them? |  |  |  |
| 9. Does training for these individuals enable them to identify and evaluate threats, vulnerabilities, and risks and understand best practices relevant to the systems components and resources for which they are responsible? |  |  |  |
| 10. Does the department encourage staff to take available cyber security awareness classes? |  |  |  |
| 11. Do all departmental staff take any “Information Technology Security Awareness” like Tutorial annually? |  |  |  |
| ***I. Publicly Accessible Computers (Computing lab, public kiosks, etc.)*** | | | |
| 1. Are the computers created with a software image configured for the greatest practicable restrictions on disk access, software installation and user rights? |  |  |  |
| 2. Are the computers refreshed frequently (daily, if possible) to force reversion to the designated software image and the removal of personal data? |  |  |  |
| 3. Are log-in IDs required? |  |  |  |
| 4. Is information posted (either by sign or log-in screen) warning users to log out of all applications, Web sessions, server connections, etc. to prevent access to their personal data by subsequent users? |  |  |  |
| 5. Are extensive anti-theft devices utilized, including locking down all peripherals and locking the computer case? |  |  |  |
| 6. Are users automatically logged-off after a short period of inactivity? |  |  |  |
| ***J. Review and Response*** | | | |
| 1. Is there a documented procedure for handling exceptions to security policies and standards? Does this procedure include higher management level review of exception approvals? |  |  |  |
| 2. Are critical systems and infrastructures, including all those storing or transmitting highly sensitive data, formally identified on a periodic basis? |  |  |  |
| 3. Do procedures for development, installation, and changes to systems and infrastructures include review and approval steps for security implications and design features? |  |  |  |
| 4. Do you have a written process for handling suspected breaches to security safeguards (e.g. intrusion detection)? |  |  |  |
| 5. Is a process in place to identify and evaluate threats and to assign appropriate action based upon risks? |  |  |  |
| 6. Does your hardware firewall technology have security logging turned on? |  |  |  |

| Prepared by:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| --- | --- |

### Step 2.2: Threat, Attack and Vulnerability Scenarios

Completion of the previous section of risk assessment questions (Step 2.1) provided a sense of current vulnerabilities. Addressing all these vulnerabilities may not be practical, however; and a way to hone in on the most vital ones to address is needed. This section guides you in thinking of these vulnerabilities in the context of potential threats and the likelihood these threats will occur. Once these connections are well understood, you will be ready to move on to development of a security plan (Step 2.3).

Below is a template for a threat-based risk assessment. It provides a checklist of strategies to deal with common threats. The information collected during this process can be plugged into and expanded upon to create (or update) your security plan (Step 2.3), identifying which strategies are already in place, which ones need to be implemented and which ones are either unnecessary or unjustifiable.

In this template, ***threats***, ***attacks*** and ***vulnerabilities*** are roughly sorted from most common to least common, which is also, fortunately, roughly least dire to most dire. Strategies to deal with the more dire threats at the end of matrix may require subsuming the strategies identified for the less dire circumstances. In those cases, feel free to refer to strategies identified previously (e.g., “see strategies for 2.B. above”) rather than duplicating information.

*Hint:* In most cases, your department’s desktops can be treated as a single item for purposes of this analysis, unless some of them uniquely host a mission-critical function.

*Note:* Do not forget paper-based data when determining which data to protect. Also, paper can serve as a backup for electronically-based data or vice-versa, assuming they are not co-located.

|  |  |  |
| --- | --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Threat, Attack and Vulnerability Scenarios  In priority order, categorize each of the assets identified in Step 1 by threat; most assets are vulnerable to multiple threats. Then identify strategies that your department *currently* follows or *plans to* follow to address these threats. | | |
| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| 1. System Software | | |
| ***A. Automated or user-initiated network-aware attacks*** (viruses, worms, trojan horses, peer-to-peer)  Consider these assets:   * Destroyed files * Exposed data * Lost productivity * Lost machine control * Lost IT staff time to rebuild machines |  | * Automatic anti-virus software updates and regular scans * Don’t open attachments * Limit use of attachments * Back up frequently * Patch applications, including e-mail clients * Managed desktop services * Configure automatic Operating Systems update and applications update * Departmental patching service * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| B. Malicious system misuse  Consider these assets:   * Ownership of shared resources (e.g. Web sites, research data) * Any resource with a password * Exposed data |  | * Effective password policies * Access controls, including access revocation ASAP but no later than one day after transfer or termination * Don’t allow applications to save passwords * Least privilege principal * Configure security settings properly, e.g. disable unused services * Implementation of a more secure network * Enforcing secure access to Internet * Enforcing web application security * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ***C. Unmanaged (uncontrolled) software installation* (**“unknown” items installed along with intended items; untested or unstable programs that interfere with supported applications)  Consider these assets:   * System reliability * Lost productivity |  | * Policies re testing software before deployment * Standard desktop configurations with limited administrator privileges * Managed desktop services * Servers administration service * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| 2. Data Integrity, Confidentiality and Availability | | |
| A. Compromise, theft and/or disclosure of databases (due to outsider cyberattack or malicious or accidental insider actions)  Consider these assets:   * Research databases * Grants * Reputation * Reproduction time * Effect on publishing (past, present, future) * Graduate student work * Financial, student, health, social security numbers and/or personnel information |  | * Prevention: see 1.B. above * Periodically compare electronic data to paper (or off-line) data (e.g. backup) * Store data encrypted * Back up frequently * Use encrypted network data transport (SecureCRT, SecureFX, ssh; VPN) * Implementation of a more secure network * Regular staff training on legal requirements and Electronic Storage of Highly Sensitive Data Policy * Follow Electronic Data Removal policy * Regularly scan with Identity Finder to remove non-essential highly sensitive data * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| --- | --- | --- |
| B. Data loss  Consider these assets:   * Any resource with electronic data storage |  | * File management practices * Back up frequently * Test backups * Off-site backup, documentation * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 3. Staffing | | |
| A. People critical to support of IT equipment/ services not available (due to illness, weather, etc.)  Consider these assets:   * IT staff |  | * Cross-training * Remote access * Documentation of procedures and practices * Common procedures across departments with partnerships for mutual backfill * Contract for backfill * Escrowed passwords * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| B. Untrained services administrators (system, database, Web, etc.)  Consider these assets:   * Servers * IT staff |  | * Hire appropriately * Provide thorough administrator training * Security training * Provide time for knowledge and skills maintenance * Provide time for on-going systems maintenance * Remote access restrictions * Strict access controls * Least privilege principal * Back up frequently * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 4. Older and Specialized Hardware and Software | | |
| A. Non-replaceable equipment (no longer manufactured); operating systems no longer supported by vendor  Consider these assets:   * Assets more than 3 years old * Specialty, unique systems |  | * Fund technology migration in coordination with vendors’ product end of life schedule * Interim manual procedures * Contingency plan for parts and emergency migration * Perform frequent, secure and tested backups * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| --- | --- | --- |
| B. “Black box” devices (non-upgradeable systems, often with unchangeable passwords)  Consider these assets:   * Specialized devices with Web interfaces (e.g. facilities control modules) * Non-computer “intelligent” devices on network; web-enabled appliances * Engineering devices |  | * Procurement contracts allowing for replacement as needed * Remove device from general network * Contingency plan for parts and emergency migration * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 5. Equipment and/or Service Unavailability | | |
| A. Unavailability of departmental IT equipment/services (due to damage from burst waterpipes, power failure, hard drive failure, confiscation by law enforcement for cybercrime investigation, denial of service attack, need to rebuild OS, human error, theft, etc.) – consider short and long term scenarios  Consider these assets:   * All assets identified in Step 1 |  | * Back up frequently * Test backups * Partnerships with other departments (instead of redundant equipment) * Service contracts * Parts on hand * Off-site backup, documentation * Interim manual procedures * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| --- | --- | --- |
| B. Unavailability of central IT equipment/services or voice communication services (due to network failure, equipment failure, denial of service attack, telecom overloads, etc.) – consider short and long term scenarios  Consider these assets:   * All assets identified in Step 1 |  | * Partnerships with other departments * Interim manual procedures * Vendor contracts for services * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 6. Loss of Facilities | | |
| A. Short term – building intact, but no access (due to structural problems, biological or chemical contamination, etc.)  ***B. Long term – building completely or substantially destroyed*** (due to fire, earthquake, missile attack, etc.)  Consider these assets:   * All assets identified in Step 1 * Paper copies of procedures, policies and plans * Local backups * Local software media and licenses * Loss of people |  | * Back up frequently * Test backups * Partnerships with other departments * Redundant equipment * Alternate space plans * Vendor contracts for services * Interim manual procedures * Off-site backup, media, licenses and documentation * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 7. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Consider these assets:   * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Prepared by: Technical contact:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

### Step 2.3: Security Plan Development

The ***aim of*** ***risk management*** is “to aid managers to strike an economic balance between the costs associated with the risks and the costs of protective measures to lessen those risks.” ***Risk mitigation*** is the actions or countermeasures taken to reduce risk.

*Countermeasure Examples*

* Fix known exploitable software flaws
* Enforce operational procedures
* Provide encryption capability
* Improve physical security
* Disconnect unreliable networks
* Train system administrators (*Train everybody!*)

A department must either take specific actions that will mitigate risks to its mission, or reject countermeasure recommendations and accept risks to its mission. Use the template below to document your decisions regarding:

1. Countermeasures you are already taking
2. Countermeasures you will implement going forward
3. Countermeasures you have identified but decided not to implement

In most risk management literature, risk is defined as

R = C x L x V (Risk = Criticality x Likelihood x Vulnerability)

The more critical the asset, the more likely the threat and the greater the vulnerability, the more risk your department faces. So you need to look at your most important assets first (identified in Step 1) and then prioritize your actions by likelihood and severity of the threats, attacks and vulnerabilities you face (identified in Step 2.2): What are the consequences to you if this happens? How can you prepare? How does the cost of preparedness compare to the cost of not acting? Then make decisions based on available resources. If resources are not sufficient, your department has prepared a case for additional resources.

The good news is that your selected strategies will often overlap; regular backup with off-site storage is a near universal strategy for threats to your assets. Also strategies do not necessarily need to be complex. For example:

* To protect all the department’s desktops: have a policy requiring all important documents be saved on the departmental file server; back up the server daily; store the backups off-site; and prepare a departmental software image for quick replacement if a desktop fails.
* To meet legal compliance standards for highly sensitive data: keep highly sensitive data on central systems, and do not download it to local servers or desktops; be in compliance by eliminating the data that would otherwise place you within the jurisdiction of the standards.

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Security Plan Template  Strategies (identified in Step 2.2) will overlap, protecting multiple assets. Document your current method of protecting assets against identified threats, attacks and vulnerabilities. Identify and prioritize what additional mitigation efforts you need to take (along with a timeline for completing them), and document justifications for mitigation steps you identified but decided not to implement. | | | |
| Asset (by priority) | Identified Threats (by priority) | | Mitigation Strategies (by priority) |
|  |  | | Current:  Planned:  Not implementing: |
|  |  | | Current:  Planned:  Not implementing: |
| Asset (by priority) | Identified Threats (by priority) | | Mitigation Strategies (by priority) |
|  |  | | Current:  Planned:  Not implementing: |
|  |  | | Current:  Planned:  Not implementing: |
| Prepared by:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

## 