**IT Security Risk Assessment**

***University of Connecticut***

<department name>

***Prepared by: , Director***

**March 26, 2008**

**Date of Last Review: March 26, 2008**

**Storage Location:**

**Primary:**

**Alternate:**

TABLE OF CONTENTS:

[ASsessment Overview 3](#__RefHeading___Toc194305285)

[Purpose: 3](#__RefHeading___Toc194305286)

[Scope: 3](#__RefHeading___Toc194305287)

[Assumptions: 3](#__RefHeading___Toc194305288)

[Location 3](#__RefHeading___Toc194305289)

[Contact Information: 3](#__RefHeading___Toc194305290)

[SCreening 4](#__RefHeading___Toc194305291)

[Risk Assessment 5](#__RefHeading___Toc194305292)

[Team Roles and Responsibilities 5](#__RefHeading___Toc194305293)

[Planning: 6](#__RefHeading___Toc194305294)

[Business Processes 7](#__RefHeading___Toc194305295)

[Systems Required: 7](#__RefHeading___Toc194305296)

[Unique Assets: 8](#__RefHeading___Toc194305297)

[Data on Stand-alone PC’s: 8](#__RefHeading___Toc194305298)

[Hardcopy Files: 9](#__RefHeading___Toc194305299)

[Files used but Owned by Other Organizations: 9](#__RefHeading___Toc194305300)

[Offsite File Storage Locations: 9](#__RefHeading___Toc194305301)

[Network Diagram: 10](#__RefHeading___Toc194305302)

[Data Flow Diagrams: 10](#__RefHeading___Toc194305303)

[Network Surveys: 10](#__RefHeading___Toc194305304)

[Previous Risk Assessment(s): 10](#__RefHeading___Toc194305305)

[Security Profile: 11](#__RefHeading___Toc194305306)

[Threat Identification: 11](#__RefHeading___Toc194305307)

[Vulnerability Identification: 11](#__RefHeading___Toc194305308)

[Current Safeguard Identification: 12](#__RefHeading___Toc194305309)

[Risk Profile: 12](#__RefHeading___Toc194305310)

[Threat Occurrence Probability: 12](#__RefHeading___Toc194305311)

[Threat Occurrence Impact: 12](#__RefHeading___Toc194305312)

[Occurrence Expected Impact: 12](#__RefHeading___Toc194305313)

[Acceptable Expected Impact Levels: 12](#__RefHeading___Toc194305314)

[Impact Statement: 13](#__RefHeading___Toc194305315)

[Additional Safeguard Options: 13](#__RefHeading___Toc194305316)

[Additional Safeguard Recommendations: 13](#__RefHeading___Toc194305317)

[Assessment Information Table: 14](#__RefHeading___Toc194305318)

[*ASsessment Maintenance Procedures:* 15](#__RefHeading___Toc194305319)

[Assessment Review and Update Process: 15](#__RefHeading___Toc194305320)

[Assessment Distribution Procedures: 15](#__RefHeading___Toc194305321)

[ADditional Documentation: 16](#__RefHeading___Toc194305322)

[Location of Supporting Documentation: 16](#__RefHeading___Toc194305323)

[*ASsessment History:* 16](#__RefHeading___Toc194305324)

[*ASsessment Sign Off* 17](#__RefHeading___Toc194305325)

# **Assessment Overview**

*Replace the “<department name>”text entries with the name of your department. Note any assumptions that apply to this risk assessment. For example, there may be areas of the department that are being excluded or organizational changes that may impact risks.*

## Purpose:

This IT Security Risk Assessment will be updated in response to changes in the business environment. The <department name> will review the assessment at least annually.

This document records the information used to assess the IT security risks for the <department name>. It includes the instructions for following the assessment process and recording the conclusions drawn from the assessment.

## Scope:

This assessment is applicable for the <department name> of the University of Connecticut.

## Assumptions:

The assumptions listed below apply to this risk assessment.

* .

## Location

*Provide the address of the department.*

University of Connecticut

…

…, Storrs, CT 06269

## Contact Information:

*Identify the people that are authorized to review or update risk assessment information.*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Primary Name & Title*** | ***Contact Data*** | ***Alternate Name*** | ***Contact Data*** |
|  |  |  |  |
|  |  |  |  |

# **Screening**

*The following questions will determine whether or not your department needs to perform an IT security risk assessment.*

*Some departments will find that their areas at risk are limited to an identifiable subset of the department. In those cases, the assessment can target the area(s) at risk and exclude areas that have no significant risks.*

*Note that many departments keep local copies of student grade reports, faculty promotion and tenure information, or other files. The primary copies of this information are usually stored and maintained in other locations, but departments that retain copies for local use are responsible for maintaining the privacy of the information.*

|  |  |  |
| --- | --- | --- |
|  | Yes | No |
| Does your department or organizational unit store or maintain data that: |  |  |
| Is subject to mandated protection under HIPAA, FERPA, or other Federal or State statutes? |  |  |
| Is any of this data classified as “registered confidential” or “confidential” as defined in the University’s Policy on Data Classification? |  |  |
| Would this data be prohibitively expensive (in terms of time, money, or other resources) to re-create if lost or damaged? |  |  |
| Does your department or organizational unit manage or support computing resources (data bases, hardware, web pages, etc.) that are used by people that access those resources from outside your department? |  |  |
| Can people access the computing equipment used by your department or organizational unit through the internet, through dial-up access, or from network devices outside your department? |  |  |
| Does any other department depend on data or computing resources that your department provides? |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*If you responded with “yes” to any of the questions, your department should complete a risk assessment as instructed in the rest of this document.*

*If you responded with “no” to all of the questions, your department does not need to complete a security risk assessment. Retain a copy of this form with your recorded answers.*

# **Risk Assessment**

*This section describes the activities for completion of an IT Security Assessment at the University of Connecticut. (This process is closely modeled after the process described in the Microsoft “Security Risk Management Guide” (which can be downloaded from* [*http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx*](http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx)*.) The guide provides extensive discussion of risk assessment concepts, processes, and tools. While the University’s process most closely follows the Microsoft guide, it incorporates process elements and tables from processes documented by NIST, SANS, CMS, and the State of Connecticut’s Department of Information Technology.*

## Team Roles and Responsibilities

*Identify the people responsible for planning and completing the assessment.*

|  |  |  |
| --- | --- | --- |
| ***Title*** | ***Name*** | ***Contact Information*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Planning:

*List the tasks that are required to complete the assessment.*

|  |  |  |
| --- | --- | --- |
| ***#*** | ***Task*** | ***Assignment*** |
| ***1*** | Develop the work plan and assign responsibilities for completing tasks. |  |
| ***2*** | Introduce team to Risk Assessment concepts, processes, and tools. |  |
| ***3*** | Review inventory of assets and resources to verify completeness. (This is trivial when the department’s Description & Inventory document is current.) |  |
| ***4*** | Use existing information to prepare the department’s **Security Profile**. |  |
| ***5*** | Identify threats to assets and resources. |  |
| ***6*** | Document vulnerabilities to those threats. |  |
| ***7*** | Document existing safeguards against threat/vulnerability combinations. |  |
| ***8*** | Prepare the department’s **Risk Profile**. |  |
| ***9*** | Document the probability of the occurrence of each threat. |  |
| ***10*** | Document the impact of a threat occurrence. |  |
| ***11*** | Prepare the department’s **Impact Statement**. |  |
| ***12*** | Define the level at which the impacts of risks become unacceptable. |  |
| ***13*** | Identify additional safeguards to be considered for safeguarding against risks that have unacceptable impact levels. |  |
| ***14*** | Select the safeguards to be recommended for implementation. |  |
| ***15*** | Document the recommended safeguards. |  |

*The material in the following sections of the assessment document is copied directly from the Inventory and Description document for this department. It presents the inventory of IT resources and assets that will be considered in this assessment.*

## Business Processes

*List the key processes performed at this location.*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Processes*** | ***Description*** | ***Frequency***  ***(daily / weekly/ monthly)*** | ***Person Performing Task*** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Systems Required:

*Provide a brief description of the computer applications and databases used at this location.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***System Name*** | ***Description*** | ***Criticality*** | ***Application Type***  ***(desktop / server / mainframe)*** | ***# Desktops Installed*** | ***Owner*** | ***Technical Contact*** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

*Criticality Ratings: 1 – The organization cannot function without the system.*

*2 – The organization can function partially without the system.*

*3 – The organization can function fully without the system.*

## Unique Assets:

*Provide a brief description of unique equipment or other major assets used at this location.*

| ***Asset Description*** | ***Qty*** | ***Vendor*** | ***Details (model #s etc.)*** | ***Criticality*** | ***Location of Asset***  ***(Campus / Building / Floor)*** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*Criticality Ratings: 1 – The organization cannot function without the asset.*

*2 – The organization can function partially without the asset.*

*3 – The organization can function fully without the asset.*

## Data on Stand-alone PC’s:

*Provide a brief description of significant data files that are kept on stand-alone PC’s at this location.*

| ***Data Description*** | ***File Name*** | ***Backup Frequency*** | ***Backup Storage Location*** | ***University Data Classification*** | ***Criticality*** | ***PC Owner*** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

*The University Data Classifications are defined in the University’s Data Classification Policy:*

*Registered Confidential*

*Confidential*

*For Internal Use*

*Public / Unclassified*

*Criticality Ratings: 1 – The organization cannot function without the data.*

*2 – The organization can function partially without the data.*

*3 – The organization can function fully without the data.*

## Hardcopy Files:

*List files that are retained on paper, microfiche, or microfilm.*

| ***Description/Name*** | ***Qty*** | ***Loc*** | ***Bldg/ Floor*** | ***Description of Contents*** | ***Criticality*** | ***Dup. Stored***  ***Offsite***  ***(yes or no)*** | ***Offsite***  ***Location*** | ***Retention***  ***Policy*** | ***Candidate for Imaging***  ***(yes or no)*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

*Criticality Ratings: 1 – The organization cannot function without the files.*

*2 – The organization can function partially without the files.*

*3 – The organization can function fully without the files.*

## Files used but Owned by Other Organizations:

*List any files that are used at this location, but are stored at another location and owned/maintained by a separate organization.*

| **Description** | **Criticality** | **Location** | **Contact Name** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

*Criticality Ratings: 1 – The organization cannot function without the files.*

*2 – The organization can function partially without the files.*

*3 – The organization can function fully without the files.*

## Offsite File Storage Locations:

*List files that are used at this location but stored at another location.*

| **Description** | **Location** | **Contact Name** | **Who has Access?** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

## Network Diagram:

*Include a diagram that shows the major components of the IT network infrastructure that supports the department. Departments that are unable to prepare this should request the diagram from the UITS Network Support Group. The diagram should show network devices and gateways, data servers, network circuits, and classes of user workstations.*

## Data Flow Diagrams:

*For each of the systems used by the department, include a diagram that shows the flow of data through the network infrastructure. The diagrams should show data moving within departmental resources, leaving the department, and coming into the department.*

## Network Surveys:

*If programs like Nessus or SARA have been used to verify the inventory of devices on the network or to assess the vulnerabilities of those devices, include a summary of the findings of the scan.*

## Previous Risk Assessment(s):

*Include a summary of the findings of previous IT Security Risk Assessments, if they provide useful input to this assessment.*

## Security Profile:

*For each of the assets and resources included in the assessment (refer to the inventory tables shown above), indicate the potential impact of loss of the resource. This is equivalent to the “exposure” level described in the Microsoft guide and the “criticality” rating in the Description and Inventory document.*

*Criticality Ratings: 1 – The organization cannot function without support are “high” impact.*

*2 – The organization can function partially without support are “medium” impact.*

*3 – The organization can function fully without support are “low” impact.*

*The profile may be simplified by grouping individual assets or resources into groups as long as the grouping definition is clearly stated.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Assets and Resources*** | ***N/A*** | ***Low*** | ***Medium*** | ***High*** |
| Sample asset |  |  |  |  |
| All systems |  |  |  |  |
| All unique assets |  |  |  |  |
| Data on individual PC’s |  |  |  |  |
| Hardcopy in lobby office and room 102 |  |  |  |  |
| Hardcopy in basement archives |  |  |  |  |
| UCHC files |  |  |  |  |
|  |  |  |  |  |

## Threat Identification:

*Review the assets and resources shown in the Security Profile and list them in the Assessment Information table. Then use the Assessment Information Table to document threats to those assets and resources. The files “Threat Table.doc” and “Common Threats.doc” provide examples of common threats.*

## Vulnerability Identification:

*Use the Assessment Information Table to document the vulnerabilities that can be exploited. The file “Common Vulnerabilities.doc” provides examples of common threats. Note that a single threat may have multiple vulnerabilities.*

## Current Safeguard Identification:

*Use the Assessment Information Table to document the safeguards that have been implemented to minimize the risks of an occurrence of each asset/threat/vulnerability combination.*

## Risk Profile:

*The marked columns of the assessment information table are the Risk Profile – documentation of the areas at risk – highlighting areas that are threatened with no current safeguards.*

## Threat Occurrence Probability:

*Record an estimated probability of occurrence for each threat occurrence. These probabilities should be in the range from 0 to 1.0 and be recorded in .1 increments (for example .7 rather than .72).*

*This assessment only requires that a probability be assigned to each threat occurrence listed. It may be useful to separately document the reasons for choosing the assigned probability value for each threat occurrence.*

## Threat Occurrence Impact:

*Record an estimated level of impact for each threat occurrence. These can be recorded on a scale from 1 to 10 (with 10 as the greatest impact) or as an estimated cost in dollars.*

*This assessment only requires that an impact level be assigned to each threat occurrence listed. It may be useful to separately document the reasons for choosing the assigned impact level for each threat occurrence.*

## Occurrence Expected Impact:

*For each threat occurrence, multiply the probability of occurrence by the estimated impact of an occurrence. This produces a relative measure of the expected impact of a threat occurrence. This measure can be compared to expected impacts of other possible occurrences without the effort required to determine precise costs of occurrences.*

## Acceptable Expected Impact Levels:

*Record the level of impact of a threat occurrence that would be acceptable to the department. This assessment only requires that an acceptable impact level be assigned to each threat occurrence listed. It may be useful to separately document the reasons for choosing the assigned level.*

*If current safeguards result in an impact estimate that is no greater than the acceptable level, no further safeguards are needed. If the current safeguards do not reduce the estimated impact to a point below the acceptable level, additional safeguards should be considered. In all cases, the “costs” associated with minimizing risk should be less than the “cost” of the threat occurrence.*

## Impact Statement:

*The marked columns of the assessment information table are the Impact Statement – documentation of the areas at risk – highlighting areas that are threatened with no current safeguards.*

## Additional Safeguard Options:

*Record any additional safeguards that could be considered for further reducing the impact of a threat occurrence.*

## Additional Safeguard Recommendations:

*Record any safeguards that are recommended for implementation to further reduce the impact of a threat occurrence.*

## Assessment Information Table:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ***Risk Profile*** | | | | ***Impact Statement*** | | | |  |  |
| ***Assets and Resources*** | ***Threat*** | ***Vulnerability*** | ***Current Safeguard*** | ***Safeguard***  ***Defense***  ***Layer*** | ***Occurrence Probability***  ***(A)*** | ***Occurrence Impact***  ***(B)*** | ***Expected Impact***  ***(A x B)*** | ***Acceptable Expected Impact Level*** | ***Additional Safeguard Options*** | ***Recommended Safeguards*** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

*Defense layers are: Physical/Administrative Probabilities are 0 to 1.0, in tenths*

*Application/System Impact Levels are 1 to 10 or dollar amounts*

*Server/Workstation .*

*Network .*

*Data .*

# ***Assessment Maintenance Procedures:***

## Assessment Review and Update Process:

*Describe the process for keeping the plan current.*

## Assessment Distribution Procedures:

*Describe the process for distributing the plan and/or training people to use its content.*

# **Additional Documentation:**

## Location of Supporting Documentation:

|  |  |
| --- | --- |
| ***Document Name*** | ***Location*** |
| ***Description & Inventory Document*** |  |
| ***Risk Assessment*** |  |
| ***PC Inventory*** |  |
| ***BCP Document*** |  |
| ***Current network diagram*** |  |
| ***Data flow diagrams*** |  |
| ***Result of network device verification scan*** |  |
| ***DoIT Security Evaluation Report*** |  |
| ***Report from Microsoft Security Risk Self Assessment*** |  |
|  |  |

# ***Assessment History:***

|  |  |  |
| --- | --- | --- |
| ***Date*** | ***RevisionSummary*** | ***Revised By*** |
|  |  |  |
|  |  |  |

# ***Assessment Sign Off***

This assessment accurately describes the information technology security risks faced by this organization. The current and recommended safeguards shown in the Assessment Information Table provide an acceptable response to the documented risks.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Director//Dean/Department Head Date**