

Facility Assessment Report   
*Unit/Department Name* -

REVISED

August 15, 2017

### Preface

This document, **Facility Assessment for Mission Critical or Essential IT Facilities** is an integral part of an IT DR Program. By taking steps to prevent a disaster or to mitigate its effects beforehand. A Facility Assessment examines various threats that could lead to a disaster, vulnerable areas, and steps taken to minimize risk to IT infrastructure and hardware that support mission critical electronic information resources and essential IT services. The threats covered in the assessment are both natural and human-created.

Other related documents include:

**Business Impact Analysis (BIA) of IT Services**

A BIA of a unit/department’s IT services is a systematic assessment of the potential impact of a loss of the service due to an interruption of computing and/or infrastructure support services resulting from a disruptive event or incident. All IT services must be included in a BIA. All IT services must be assigned a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) by their information resource owner.

**Department/Unit IT Disaster Recovery Plan (IT DRP)**

IT DRP is focused on the overall recovery of IT services based on the information resource owner’s established Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Detailed recovery procedures and assumptions of individual or a group of interdependent mission critical electronic information resource or essential IT services are stored in the department/unit’s Information System Contingency Plan(s) (ISCP).

**Information System Contingency Plan (ISCP) for Mission Critical / Essential IT Services.**

IT Services that have been identified by the information resource owner or the Chief Information Security Officer (CISO) as either an essential IT service or a mission critical electronic information resource must be included in an ISCP. An ISCP can be completed for an individual IT service or a group of interdependent IT services. AnISCP contains detailed procedures to recover a ***mission critical or essential IT service*** or a grouping of interdependent IT services following a disruption. Mission critical electronic information resources and essential IT services must be exercised annually.

**Cost Benefit Analysis Reports**

A Cost Benefit Analysis is only required if the IT service is determined to be an essential IT service and the actual Recovery Time Objective (RTO) is not in alignment with the required RTO.

**Texas A&M University IT Disaster Recovery Plan (DRP)**

Texas A&M University IT DRP, explains how the university recovers Essential IT Services following an emergency or disruption. The Texas A&M University IT DRP is written in support of  [Annex J](https://www.tamu.edu/emergency/documents/AnnexJ.pdf) (Institutional Continuity Plan) of the [Texas A&M University Emergency Operation Plan](https://www.tamu.edu/emergency/documents/EOP.pdf).. Organizations supporting the Essential IT Services shall maintain their own procedures and actively participate in the training, exercise, and maintenance needed to support this plan.

### Approval

*<Provide a statement in accordance with the unit/department’s contingency planning policy to affirm that the Facility Assessment is complete. This statement should be approved and signed by the Information Resource Owner. Space should be provided for the Information Resource Owner(s) to sign, along with any other applicable approving signatures. A sample language is provided below: >*

The Information Resource Owner acknowledges the results of the Facility Assessment Report.

Approved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name

Title

Unit/Department Name

**Note to the Author**

This document can be used as a template for a Facility Assessment. This template includes instructions to the author, boilerplate text, and fields that should be replaced with the values specific to the project.

Red *italicized text enclosed in angle brackets* (<text>) *provides instructions to the document author, or describes the intent, assumptions and context for content included in this document. Delete the blue text as you fill out the document.*

Blue *italicized text enclosed in square brackets* ([text]) *indicates an example/field that should be replaced with information specific to a particular project.*

Text and tables in black are provided as boilerplate examples of wording and formats that may be used or modified as appropriate to a specific project. These are offered only as suggestions to assist in developing project documents; they are not mandatory formats.

Table of Contents

[Overview 6](#_Toc490473539)

[Locations 6](#_Toc490473540)

[Floor Plans 7](#_Toc490473541)

[*Location 1* Assessment Form 8](#_Toc490473542)

[Index 15](#_Toc490473543)

[Record of Change 16](#_Toc490473544)

# Overview

An integral part of an IT disaster recovery plan (DRP) is taking steps to prevent a disaster or to mitigate its effects beforehand. This portion of the plan examines various threats that could lead to a disaster, our vulnerable areas, and steps taken to minimize our risk. The threats covered here are both natural and human-created.

Organization-wide risk mitigation activities. These include, but are not limited to, monitoring and control activities, scheduled maintenance on hardware and infrastructure, testing and installing software patches, and regular testing of backups.

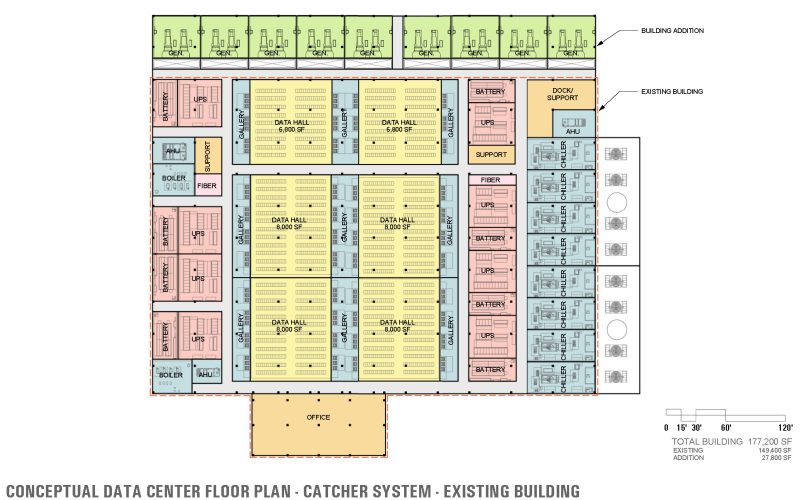
A facility assessment is only required for sites that support essential and mission critical IT Services.

## Locations

|  |  |
| --- | --- |
| **Location Name 1** | |
| Building Number | # |
| Staffed | 24/7, Office Hours, lights out, |
| Run time on Batteries | # Minutes. |
| Run time after the loss of building HVAC | # Minutes. |
| Environmental Monitoring System | NetBotz, ect. |
| Generator | Dedicated / Life Safety |
| Fully redundant Backup HVAC System | Yes / No |
| Area Maintenance Zone | # |
| Square Feet | # |
| Number of Racks | # |
| Number of Servers | # |
| Number of Blade Servers | # |
| Energy Management POC | Name |
| Building Proctor | Name |
| Room Proctor | Name |
| Managing Unit/Department | Name |
| CoLocation Partners | Unit/Department Name |
| External Maintenance Vendors | Computer, HVAC, Electrical, ect. |

# Floor Plans

*EXAMPLE of Floor Plan BELOW*



# *Location 1* Assessment Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Location Assessment Form** | | | | |
| **Required** | **Number** | **Question** | | **Requirement** |
|  | **1** | **Department Name** | |  |
| \* |  |  | |  |
|  |  |  | |  |
|  | **2** | **Building Name / Number** | |  |
| \* |  |  | |  |
|  |  |  | |  |
|  | **3** | **Room Number** | |  |
| \* |  |  | |  |
|  |  |  | |  |
|  | **4** | **Infrastructure Location Manager** | |  |
| \* |  |  | |  |
|  | | | |  |
| **Access Controls** | | | |  |
|  | **5** | **How many layers of physical security are present before you can access facility from public space? \*** | |  |
|  |  |  | |  |
|  |  |  | |  |
|  | **6** | **Describe the layers of physical security in detail. Do not include access controls.** | |  |
|  |  |  | |  |
|  |  |  | |  |
|  | **7** | **What type of access controls are present on doors?** | |  |
|  |  | Mark all that apply. | |  |
|  |  |  | Key lock |  |
|  |  |  | Card Swipe |  |
|  |  |  | Biometric |  |
|  |  |  | Smart card |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **8** | **Are there documented policies and supporting procedures to protect the facility as necessitated by its criticality?** | | **TAC PE1** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  | Comments: | |  |
|  |  |  | |  |
|  | **9** | **Has the physical environment been tested for potential circumvention measures?** | | **TAC PE16** |
|  |  | **Have all ingress/egress points been assessed** | |  |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  | Comments: | |  |
|  |  |  | |  |
|  | **10** | **Has the organization implemented Physical Access Safe Guards?** | | **TAC PE1** |
|  |  | See other question regarding types of safeguards. | |  |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  | Comments: | |  |
|  |  |  | |  |
|  | **11** | **Choose all applicable descriptions for what the access controls do:** | | **TAC PE1** |
|  |  | Take into account external utilities used to provide AC. | |  |
|  |  | Mark all that apply. | |  |
|  |  |  | Grant access |  |
|  |  |  | Control access |  |
|  |  |  | Monitor access and provide auditable log |  |
|  |  | Comments: | |  |
|  |  |  | |  |
|  | **12** | **Does the organization maintain a list of authorized personnel that is approved by an executive business owner or delegate?** | | **TAC PE2(a)** |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  | Comments: | |  |
|  |  |  | |  |
|  | **13** | **Describe the authorization mechanism for facility access** | | **TAC PE2(b)** |
|  |  | Mark all that apply. | |  |
|  |  |  | Local controlled access mechanism (LDAP/AD/equivalent) |  |
|  |  |  | No automated mechanisms |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **14** | **How often is the Authorized Personnel List reviewed and modified?** | | **TAC PE2©** |
|  |  | Mark all that apply. | |  |
|  |  |  | Daily |  |
|  |  |  | Weekly |  |
|  |  |  | Monthly |  |
|  |  |  | Yearly |  |
|  |  |  | It is not updated |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **15** | **15. How soon are individuals removed from the Authorized Personnel List after access is no longer required?** | | **TAC PE2(d)** |
|  |  | Mark only one box. | |  |
|  |  |  | Immediately (within 1 business day) |  |
|  |  |  | Within a week |  |
|  |  |  | Within two weeks |  |
|  |  |  | Within a month |  |
|  |  |  | Within a month |  |
|  |  |  | Within 6 months |  |
|  |  |  | Within a year |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **16** | **16. Do individuals has to be authenticated both on ingress AND egress** | | **TAC PE3(a)** |
|  |  | Mark all that apply. | |  |
|  |  |  | Ingress/Entry |  |
|  |  |  | Egress/Exit |  |
|  |  |  | No required authentication (public access) |  |
|  |  |  | |  |
|  | **17** | **17. Are auditable logs maintained for physical access to facility?** | | **TAC PE3(b)** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  | Comments: | |  |
|  |  |  | |  |
|  | **18** | **18. If there are audible logs, where are they stored** | | **TAC PE3(b)** |
|  |  | Mark all that apply. | |  |
|  |  |  | Within the access mechanism's database |  |
|  |  |  | Backups/regular data dumps |  |
|  |  |  | Syslog or equivalent server |  |
|  |  | Other: | |  |
|  |  |  | |  |
| **Visitors** | | | |  |
|  | **19** | **Are visitors monitored by authorized personnel?** | | **TAC PE3(d)** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **20** | **How regularly are visitors allowed access without full supervision** | | **TAC PE3(d)** |
|  |  | **Mark only one box.** | |  |
|  |  |  | Never |  |
|  |  |  | Rarely |  |
|  |  |  | Sometimes |  |
|  |  |  | Often |  |
|  |  |  | Always |  |
|  |  |  | |  |
|  | **21** | **Are visitors logged or required to signin before entry?** | | **TAC PE8(a)** |
|  |  | **Mark only one box.** | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **22** | **How are visitors logged?** | | **TAC PE8(a)** |
|  |  |  | Paper log |  |
|  |  |  | Computer-based |  |
|  |  |  | log |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **23** | **How often are the visitor logs reviewed?** | | **TAC PE8(b)** |
|  |  |  | Daily |  |
|  |  |  | Weekly |  |
|  |  |  | Monthly |  |
|  |  |  | Yearly |  |
|  |  |  | As needed/infrequent |  |
|  |  | Other: | |  |
|  |  |  | |  |
| **Key Management and Security Incident Response** | | | |  |
|  |  |  | |  |
|  | **24** | **Describe how keys and other physical access controls are protected and stored.** | | **TAC PE3€** |
|  |  |  | |  |
|  | **25** | **When keys are lost or stolen, are the associated locks changed?** | | **TAC PE3(g)** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **26** | **Are access control mechanism outputs protected from access by unauthorized individuals** | | **TAC PE5** |
|  |  | Are auditable logs protected | |  |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **27** | **How regularly are auditable access control mechanism logs reviewed for potential incidents?** | | **TAC PE6(a)** |
|  |  | Mark only one box. | |  |
|  |  |  | Daily |  |
|  |  |  | Weekly |  |
|  |  |  | Monthly |  |
|  |  |  | Yearly |  |
|  |  |  | Never |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **28** | **When a physical security incident is detected, are the logs reviewed?** | | **TAC PE6(b)** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **29** | **Which authorities are contacted in the event of a Physical Security Incident** | | **TAC PE6©** |
|  |  | Mark all that apply. | |  |
|  |  |  | Police/Campus Security |  |
|  |  |  | Office of the CISO (Incident response) |  |
|  |  |  | Office of General Council (OGC) |  |
|  |  | Other: | |  |
|  |  |  | |  |
| **Electrical Protection** | | | |  |
|  |  |  | |  |
|  | **30** | **Provide a brief description of how power cabling and equipment are protected:** | | **TAC PE9** |
|  |  |  | |  |
|  |  |  | |  |
|  | **31** | **Is there an Emergency Power Shutoff? Cuts power immediately.** | | **TAC PE10(a)** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes, bypasses facility UPS |  |
|  |  |  | Yes, does not bypass facility UPS |  |
|  |  |  | Yes, does not bypass rack/system UPS |  |
|  |  |  | Yes, bypasses rack/system UPS |  |
|  |  |  | No. There is not an emergency power shutoff |  |
|  |  |  | |  |
|  | **32** | **If applicable, is the emergency shutoff placed in a convenient location for personnel** | | **TAC PE10(b)** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | Yes, and easy to access on egress |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **33** | **How is the emergency shutoff protected from unauthorized access?** | | **TAC PE10©** |
|  |  | Mark only one box. | |  |
|  |  |  | Key lock |  |
|  |  |  | Not protected |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **34** | **Mark all that apply regarding short term UPS:** | | **TAC PE11** |
|  |  | Mark all that apply. | |  |
|  |  |  | Facility wide UPS |  |
|  |  |  | Rack-wide UPS |  |
|  |  |  | System level UPS |  |
|  |  |  | Automated control software and procedures for graceful shutdown |  |
|  |  |  | Tiered-service shutdown automated procedures |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **35** | **Is there emergency lighting in the case of a power outage?** | | **TAC PE12** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
| **Fire Suppression and Environmental Protection** | | | |  |
|  |  |  | |  |
|  | **36** | **Is a fire suppression system installed?** | | **TAC PE13** |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **37** | **Describe the fire suppression system:** | | **TAC PE13** |
|  |  | Mark all that apply. | |  |
|  |  |  | Halon |  |
|  |  |  | Water sprinkler |  |
|  |  |  | Oxygen reduction |  |
|  |  |  | Fire alarm |  |
|  |  | Other: | |  |
|  |  |  | |  |
|  | **38** | **Are temperatures and humidity levels monitored and maintained?** | | **TAC PE14** |
|  |  | Mark all that apply. | |  |
|  |  |  | Temperature |  |
|  |  |  | Humidity |  |
|  |  |  | No |  |
|  |  |  | |  |
|  | **39** | **Is the facility susceptible to water damage?** | | **TAC PE15** |
|  |  | Like busted pipes overhead | |  |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | Maybe/Unknown |  |
|  |  |  | Fire alarm |  |
|  |  |  | |  |
|  | **40** | **Are there accessible shutoff valves for pipes within the vicinity of the facility?** | | **TAC PE15** |
|  |  | If a leak happens, are there shutoff valves? | |  |
|  |  | Mark only one box. | |  |
|  |  |  | Yes |  |
|  |  |  | No |  |
|  |  |  | |  |

# Index

**No index entries found.**

# Record of Change

This plan is updated at least annually, as described in the ISRR Program document.

|  |  |  |  |
| --- | --- | --- | --- |
| **RECORD OF CHANGE** | **DATE OF**  **CHANGE** | **DESCRIPTION OF CHANGE** | **CHANGE MADE**  **BY:** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |