**RISK MITIGATION PLAN FOR IPADIUM**

This risk mitigation plan is one component of the overall risk management process for mitigating the risks associated with ipadium.

**Mitigation Plan**

This Risk Mitigation Plan organizes the mitigation activities in view of the presentation element of every vulnerability. The nearer to the end client in which the vulnerability lies, the more probable the vulnerability could effectively be abused. Prescribed points of reference are incorporated to give an underlying pattern to staging the mitigation activities. Endorsement of the relief stages, planning, and assets will be expert by means of the IT Governance process.

The following are the vulnerabilities accepted and also the vulnerabilities required to mitigate which are accepted by a senior leadership:

1. **ACCEPT:**

* **Access Control (AC)**
* **Awareness and Training (AT)**
* **Audit and Accountability (AU)**
* **Configuration management (CM)**
* **Identification and Authentication (IA)**
* **Contingency planning (CP)**
* **Incidence response (IR)**
* **Physical and Environmental Protection (PE)**
* **Risk assessment (RA)**
* **System and Information Integrity (SI)**

1. **MITIGATE:**

* **Awareness and Training (AT)**
* **Audit and Accountability (AU)**
* **Identification and Authentication (IA)**
* **Awareness and Training (AT):**

Security Policy preparing in many organizations concentrates on acquainting the workers with the hierarchical security approach. The security mindfulness center for clients may include:

* Educating clients on the making of good passwords.
* Do's and don'ts for keeping up workstations.
* Informing clients of email and Internet access approaches.
* Employee obligation regarding PC security.

The best difficulties that the organizations are confronting today is in building a security mindfulness program i.e. where to begin, how would you arrange, create, convey, and how you can keep up a viable mindfulness program. For that we have different assets to help you arrange and keep up a mindfulness program that is agreeable, as well as connects with your representatives and spotlights on diminishing danger by changing their practices.

* [Gaining Internal Support](http://securingthehuman.sans.org/resources/getting-support)
* [Planning Your Awareness Program](http://securingthehuman.sans.org/resources/planning)
* [Measuring Results](http://securingthehuman.sans.org/resources/metrics)
* **Gaining Internal Support:**

Many associations face is getting administration endorsement and/or subsidizing for their mindfulness program. This segment contains assets to legitimize and get support for your own mindfulness program. The Stake holder presentation can be utilized to present to your senior administration to clarify the estimation of your proposed security mindfulness program; giving you the bolster, spending plan and assets you have to make your mindfulness program happen.

* **Planning Your Awareness program:**

The long term challenges confronted by any mindfulness project is inspiring it to stick. We clarify what associations are successfully doing the world over to candidly connect with and impart to their representatives. Key focuses you will learn incorporate conduct displaying, characterizing society, building up an engagement procedure, specialized techniques and envoy programs.

* **Measuring Results:**

Measurements give you the capacity to track and measure the effect of your security mindfulness program. This can be utilized to enhance your preparation, exhibit degree of profitability, or contrast your human danger with different associations in your industry.

* **Audit and Accountability (AU):**

The organization routinely surveys/examines review records for signs of unseemly or abnormal action, researches suspicious movement or suspected infringement, reports discoveries to suitable University authorities and takes important activities.

Non-renouncement administrations can be utilized to figure out whether data began from an individual or if an individual took particular activities (e.g., sent an email, marked an agreement, affirmed an acquirement ask for) or got particular data and these are also acquired by utilizing different strategies or components (e.g., computerized marks, advanced or digital message receipts, time stamps).

Non-renouncement secures against false claims by:

* a creator of not having composed a specific archive
* a sender of not having transmitted a message
* a collector of not having gotten a message
* a signatory of having marked a record

The association indicates which data framework segments do inspecting incidents. Examining movement can influence data framework execution. Along these lines, the association chooses, based upon a danger appraisal, which occasions require evaluating on a constant premise and which occasions require reviewing in light of particular circumstances. The association characterizes auditable occasions that are satisfactory to bolster afterward examinations of security incidents. The following are some of the control enhancements which are required:

* The organization utilizes robotized systems to incorporate review checking, examination and reporting into a general procedure for examination and reaction to suspicious exercises.
* The organization utilizes robotized systems to instantly ready security work force of unseemly or strange exercises that have security suggestions.
* **Identification and Authentication (IA)**:

System Owners (SO), in coordination with Information Security Officers (ISO), Information Management Officers (IMO), Information Owners (IO), Information System Security Officers (ISSO), Common Control Providers (CCP), and Security Control Assessors (SCA), for EPA-operated systems shall; and Service Managers (SM), in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure some service providers:

* Design data frameworks to exceptionally recognize and validate clients (or forms following up in the interest of clients).

Users might be exceptionally recognized and validated for all entrance other than those gets to unequivocally recognized and recorded as exemptions in regards to allowed activities without recognizable proof and verification.

* Refer to the most recent variant of the EPA Information Security – Access Control techniques for prerequisites on allowed activities without distinguishing proof and verification.
* Unique distinguishing proof of people in gathering accounts (e.g., shared benefit records) may not be required for itemized responsibility of movement depending upon dangers. SOs should base their proposal to not utilize one of a kind identifier for people in gathering accounts on a danger appraisal.
* Implement recognizable proof and confirmation instruments at the application level, as controlled by a danger evaluation, to give expanded security to the data framework and the data forms. This might be notwithstanding distinguishing and validating clients at the data framework level (e.g., when at first signing into a desktop, tablet or advanced mobile phone).
* Authenticate client characters using passwords, individual recognizable proof numbers (PINs), tokens, biometrics, or on account of multifaceted validation, a few blend thereof.

The vulnerabilities after mitigation and its requirements are explained in the following table in which the risk levels are different for different vulnerabilities.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Risk Level** | **Vulnerability** | **Mitigation Decision** | **Mitigation Actions** | **Estimated Resources Required** | **OPR** | **ECD** |
| 1 | High | **Awareness and Training**:  Focus attention on policies and associated procedures i.e. the users of organizational systems are to be aware of the risks associated with their activities and applicable laws.  Ensure that organizational personnel are well trained to carry out their assigned duties. | Y | Awareness presentations are intended to allow individuals to recognize information and security concern, Awareness Team conducting sessions should have knowledge from all the departments and policies (Ex: IT, Security, Network etc.) | Dedicated team who will conduct sessions regularly on latest updates.  Tools which provide help in conducting awareness.  $2000 and Man hours, can be every month depending on the implementation on new programs, policies and information. | Human Resource, Finance Department  Management to approve. | As this needs to be implemented each time on a new information, it’s a  continuous process |
| 2 | Moderate | **Audit and Accountability:**  The purpose of this is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. | Y | **Technical:**  Implement automated log tools, Audit trails helps to maintain individual accountability. | $349 for auditing tool (Loggly)  20 man hours to implement. | Security, IT, Admin department. | 05/16/2016 |
| 3 | Low | **Identification and Authentication:** Organizations must have to identify the IT system users and has to process them on behalf of the users and need to authenticate the identity of those users. | Y | Identify security systems, validate user identify, identify security authority, secure code writing techniques and input parameters, password salting. | 14 hours to implement changes and test the system. | Server and database  admin  system admin | 06/08/2016 |