System Security Measures

Implementation of Security for Project Development

## PURPOSE OF THESE MEASURES

These Measures apply to anyone who accesses, uses, or controls Project, computer and data resources. The measures also apply to the users of the system, project and resources.

## SCOPE OF THESE MEASURES

These Measures are applicable to a wide variety of IT resources which are are used for project purpose. A system may be any IT resource. Examples of systems include, but are not limited to: Workstation (Computers, laptop, server, OS), Mobile Devices, Network, Server, Web application, Databases.

All of the above systems may perform their own authentication and authorization, logging and auditing, and have their own configurations which must be managed, and each of them are considered a compliance object to be protected.

## SYSTEM SECURITY MEASURES

## **Password Protection:** All accounts and resources are be protected by passwords which meet the following requirements, which must be automatically enforced by the system:

* + Must be at least eight characters long
  + Must NOT be dictionary or common slang words in any language, or be readily guessable
  + Must include at least three of the following four characteristics in any order:upper case letters, lower case letters, numbers, and special characters, such as\*!@#$%^&\*.
  + Must be changed at least once per year.

**Antivirus :** Antivirus acts as the first line of defense against security attacks and prevents them from causing damage to your sensitive data. It takes care of a variety of security threats such as malware, viruses, spyware and adware. Some even offer email protection and prevent harmful downloads.

**Regular Backup of Data :** Regular backup of Project Data will help to protect against one of the most common cyber attacks today, Ransomware. Even if a cyber attack targets the system, it be easy to restore and reclaim data if there is a backup ready. Cloud storage can also be used to make copies of data and store it there. Schedule of regular backup to protect and keep data safe will help to prevent of precious Project data loss.

**Software Updates**: Systems are configured to automatically update operating system software, server applications (webserver, mailserver, database server, etc), client software (web-browsers, mail-clients, office suites, etc), and malware protection software (anti-virus, anti-spyware, etc). For *Medium* or *High Availability* systems, a plan is framed to manually apply new updates within a documented time period is also performed as an acceptable alternative.



**Authentication and Authorization**

Following are the measures taken into account :

**Remove or disable accounts upon loss of eligibility**: Accounts which are no longer needed are disabled in a timely fashion using an automated or documented procedure.

**Separate user and administrator accounts**: Administrator accounts are not be used for non-administrative purposes. System administrators are provisioned with non-administrator accounts for end-user activities, and a separate administrator account that is used only for system-administration purposes.

**Use unique passwords for administrator accounts**: Privileged accounts will use unique passwords that are not shared among multiple systems.

**Enforce least privilege**: Non-administrative accounts are used whenever possible. User accounts and server processes are granted the least-possible level of privilege that allows them to perform their function.

**Configuration and Maintenance**

**Security Partitioning**: Systems will share hardware and resources only with other systems that have similar security requirements, regardless of their *criticality* classification.

**Follow vendor hardening guidelines**: All softwares used are open source and in other case if not licenses are obtained.

**Disable all unnecessary network services**: Processes and services which are not necessary to complete the function of a system are disabled.

## DATA HANDLING SECURITY MEASURES

## These Data Security Measures define the minimum security requirements that are applied to the data types defined in System Classification. Some data elements, such as credentials have additional security requirements defined in external standards.

## **Requirements Handling Confidential Data**

## **Access control**: Access to *confidential data* is provided on a least-privilege basis. No person or system will be given access to the data unless required by business process. Access to *protected data* is provided on a least-privilege basis. Restricted data will only be collected when all of the following conditions are met:

## The data is not available from another authoritative source, and The data is required by business process

## **Sharing**: *Confidential data* will be shared among the University department heads.

## **Retention**: *Confidential data* will only be stored for as long as is necessary to accomplish the documented business process.

## **Storage encryption**: Restricted data is encrypted using strong, public cryptographic algorithms and reasonable key lengths given current computer processing capabilities. Keys are stored securely, and access to them provided on a least-privilege basis.