Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

Access Control Standard Operating Procedure

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			MOITT	**1.0**	

Change History

SN	Version	Changes Description
1	**1.0**	**Final Version**

Table of Contents

1 Abbreviations

IIS: Internet Information Services

NTP: Network Time Protocol

PSTN: Public Switched Telephone Network

2 Introduction

Adequate physical and logical security is mandatory for all information assets. Physical structures should be secured from both covert and overt penetration. Following policies shall be implemented as general principle for access control. Role and personal based logical access control should be practiced. Authorization levels will be based on job requirements.

3 Scope

The Access Control SOP applies to all employees, non-employees and consultants. The policy also applies to all users that have been granted the access of the physical premises and Information Technology resources.

4 Purpose

Access to Information Technology resources is granted in a manner that carefully balances restrictions designed to prevent unauthorized access against the need to provide unhindered access to informational assets. The purpose of the document is to describe Standard Operating Procedures for the secure access to information technology resources and its premises.

5 The Policy

All employees and other users will be provided with the information they need in order to carry out their responsibilities in as effective and efficient manner as possible.

Users are expected to become familiar with and abide by these policies, standards and guidelines for appropriate and acceptable usage of the information technology resources. Every user must maintain the confidentiality of information assets.

Employees should follow the below mentioned rules: -

1. Access to private information will be limited to authorized persons whose job responsibilities require it, as determined by an appropriate approval process.
2. Access will be given through the establishment of a unique account in accordance with account request procedures.
3. Managers shall arrange for obtaining and granting the security identification of temporary employees and visitors who access secure area.

4. All personnel are responsible for ensuring that unauthorized individuals are not permitted access to restricted areas. In restricted areas, all personnel are required to display badges in a manner that is easily observed by all.

5. Highly sensitive information assets shall be protected using accountable access control.

6. Managers should perform unscheduled assessments of physical access control.

7. All server systems containing essential or highly sensitive information assets must be located inside secure and accountable areas.

8. All physical areas containing information assets will meet or exceed standards for fire, water, electric power faults, physical damage, environmental, and theft protection.

9. Video camera's operated for surveillance or monitoring must ensure compliance with law.

5.1 System Monitoring

1. Where system logs are used for monitoring there must also be procedures and responsibilities in place to audit the logs. However, because of the significant amount of work involved in this type of monitoring, and the increasing speed and sophistication of attacks, it may be more appropriate to use specialized software such as SIEM. The Rules of Evidence might also require consideration when choosing the type of logs to be collected and the data items to be in them. System logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorization and strict authentication.

2. An example of a monitoring standard is as follows:

   a. Review/scan for any usage of any utility tool like PSExec within the network in the last two months.

   b. Ensure proper configuration of the Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network. In addition to any VPN logs.

   c. Ensure that alerts are generated for all suspicious activity on the network (e.g. port scanning, remote connections, using local administrator accounts over the network).

   d. Configure all IIS logs, and other similar systems, to log the external IP instead of the load balancer/proxy internal IP.

   e. Backup security related logs to secure offline location where possible.

   f. Perform regular scanning for unauthorized software. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives.

   g. Monitoring records (audit trails) should include user identifiers, dates and times for logon and logoff, terminal identity or location, the programs executed, the files accessed; and the program and/or session completion status.

5.2 Clock Synchronization

1. The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

2. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, such as Greenwich Mean Time (GMT) or local standard time. Clocks tend to drift from the correct time over time, so the devices should be set with the local NTP Server.

5.3 Mobile Computing

1. When mobile computing is employed the risks of compromise, the remote site must be considered, as must be the vulnerability of data interception and of unauthorized access into the organization's internal network through the remote access path.

2. There are a huge number of laptop computers lost and stolen every year. Therefore, additional physical protection such as cable locks may be considered for equipment in open or shared environments where it cannot be monitored at all times. In situations where unauthorized users might gain access to the computing equipment removable media should be used and secured when the equipment is vulnerable, or encryption should be considered. Protection for sensitive or classified hard copy output should also be considered at the remote sites.

3. File or communications encryption should be employed when transferring sensitive information across a public network (e.g. the PSTN or the Internet).

4. Most products also include strong authentication services, which will reduce the risk of unauthorized access to the organization's network via the remote access service compared with password authentication. Passwords should never be passed 'in the clear' and a second level of authentication should be employed (2FA) where possible.

5. The remote access entry point into the organization's network should be configured and managed very carefully. Only those services required by the remote workers should be available through this communications path. The remote access capability should only be activated when it is needed and only for those users that need it. It should follow the authorization process and access acknowledge form must be signed. Audit logs should be monitored to detect unauthorized access attempts. Remote workstations should also have a virus checking capability.

5.4 Privilege Access

1. The requirement and level of privileged access associated with each system, and the categories of staff to which privileged access is to be allocated, must be predefined and approved.

2. Privileged access must be allocated to individuals on a "need-to-use" basis and on an "event by event" basis.

3. Access to system resources such as source code, application development environments and configuration files should also be controlled.

5.5 Administrative Rights

1. The granting of administrative rights allows the individual to change the configuration settings of a given machine and install software on that machine. As a result, these rights can expose the network to malware and other security exploits. In addition, incorrect configuration of machines can lead to performance problems, potentially resulting in machine downtime, lost productivity, and higher support cost.

2. Given the serious consequences of mishandling or abuse of administrative rights, these rights will only be granted under the condition that they are essential for the performance of the grantee's job. Such conditions could include the following:

   a. The ability to download and install specific types of software or configure system settings is mandated in the individual's job description.

   b. An administrative rights access level is required for a necessary software title to run on given machine.

   c. Sufficient levels of IT support do not exist due to time-of-day, geographical, or expertise constraints.

   d. For providing PC support.

Typically, the members who are granted administrative rights should be properly documented in Administrative Group.

Note: Members of a department are not automatically granted administrative rights based on their membership in the alone.

If you do not assign as per Administrative group and believe it is required by your job then you will need to raise a request for the approval of administrative rights. The designated authorities reserve the right to deny the request if it does not represent a clear business need or if the applicant has a documented history of information security policy violation.