IT Access Control Policy

Version History:

Ver. No.	Release Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
0.1	3rd Sep 2013	First Draft	Saket Madan	Dhananjay Kumar	Ajay Kumar Zalpuri
1.0	30th Sep 2013	Initial Release			
1.1	17th May 2019	Update section1 for objective and update section 3.3	Saket Madan	Dhananjay Kumar	Ajay Kumar Zalpuri

Table of Contents

1. Objectives

The purpose of this document is to explain organization's access control policies for:

- Access to premises
- Access to systems (employee machines as well as servers), Cloud System and Network
- Access to Operating system

2. Scope

Access control includes managing remote access and enabling administrators to be efficient in their work. The policy applies to all the employees, vendors, business partners, and all those who work with the information processing systems and facilities of NST.

3. Policy

IT Head has identified best practices for access control to Server room, systems, network, and applications. These best practices are categorized as follows:

- Security Logging and Monitoring
- Access Control to Server room
- Access Control to Network and Systems (which includes user account management and privileges management)

3.1 Security Logging and Monitoring Guidelines

System Logging and Monitoring guidelines aim at detecting unauthorized activities being performed or any such attempt of unauthorized access.

- IT Team will ensure the maintenance of a log of security events.
- Authorization by the Manager IT will be required in case of exceptions to the logging and the same will have to be recorded.
- All activities done (like file access/deletion/modification etc.) by an administrator on an Organizational Server after successfully logging into the system will be logged.
- All servers will be configured to enable logging of system events related to security.
- IT Head will formulate appropriate procedure to ensure that the critical servers are reviewed on a regular basis to identify any malicious code installed or executed.
- The periodic review will also focus on whether the service packs and version installed are up-to-date or not.

3.2 Access Control to Server Room

- A register is kept logging the details of visitors entering the server room.
- Each employee has also been issued an 'ID Card'. This 'ID Card' will have a photograph of the employee along with the employee's name and employee ID.

3.3 Access Control to Network and Systems

- All users are assigned rights and permissions based on the requirements of the roles and responsibilities they hold to perform their duties in NST.
- All machines have inbuilt security system which automatically locks the machine if employee leaves the machine idle for a specific period (which is 5 minutes).
- All the users requiring access to NST network and the network are assigned unique user accounts and associated passwords.
- All user accounts created and maintained on NST IT systems follow a standard naming convention.
- All new user accounts to be created by the IT department when HR sends email. And IT department shall remove the access from Active Directory when personnel leaving informed by HR.
- IT department will be responsible for user account creation/deletion/disabling and maintaining the records for all the user accounts created/deleted/disabled from the IT systems of NST.
- IT department will be responsible for organizing user accounts in groups formed based on the various roles and responsibilities assigned. Users will also be grouped as per their respective departments.
- The allocation and revocation of privileges must be controlled through a formal authorization process. (VPN, Licensed Software Installation, Bandwidth/Web-access level increase, Approval Processes).

3.4 Operating System Access Control Guidelines

- All successful and failed login access to server shall be logged along with login name, date, and time.
- Appropriate limited access permission shall be configured on file system/partition/directory to restrict unauthorized access.
- A general notice warning shall be displayed while terminal log-on process. The log-on banner needs to be clearly state that following:
    - Unauthorized access is prohibited
    - Usage of this system is being monitored and disciplinary action would be taken for any misuse

System administrator shall ensure 24x7 availability of servers.