Access Control and Password Policy

Purpose

Chattr implements physical and logical access controls across its networks, IT systems and services in order to provide authorized, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy. Access control systems are in place to protect the interests of all authorized users of Chattr by providing a safe, secure and accessible environment in which to work.

Scope

This system specific policy covers the Chattr system, networks, data, and how this is used. The Chattr system is only accessible by authorized users.

Roles and Responsibilities

System Owners

Individuals who have responsibility for systems (including designating access) upon which Chattr's data reside and within a given area for information systems in use in this area, those individuals has the primary responsibility for ensuring compliance by all Chattr users with the following principles:

- Ensuring correct security measures are in place to protect employee and customer's information and personal identifiable records
- Establishing the roles and access levels for the system.
- Approving or denying all access request to their system.
- Maintaining correct administrative processes to ensure system information is accurate.
- Any future developments of Chattr are undertaken in line with the organization's business needs and information policies and adhere to change control processes
- Appropriate application support is in place with Chattr e.g. performance and service level agreements - and closely monitored including renewal of license and support arrangements in a timely manner

Department of Information Management and Technology

- Administering access to Chattr Active Directory environment and many of its systems
- Responsible for approving information security policies
- Hardening end user systems in accordance with research data provider requirements
- Implementing role based access control upon the Chattr's shared access file systems,
- Creating Chattr's Active Directory user accounts and passwords.
- Maintaining Chattr's network infrastructure, firewalls and network zoning.
- Maintaining the External Contractors Access Framework.
- All members of staff that require access to Chattr have received the necessary training in the use of Chattr and have been provided with a unique log on and password.
- Technical Operating Instructions are in place for the maintenance and upkeep of the Chattr server and Chattr system administration tasks.

Information Security Manager

Responsible for writing this policy and establishing access control principles, such as:

- New users are correctly added to the system configuration and given the correct authorized permissions to operate Chattr and appropriate user forms are completed
- System users who no longer require access or who have not logged into the system for 90 days have their accounts disabled in a timely manner
- System users who no longer require access to a module within Chattr have their user account permissions modified

Information Security Team

Responsible for:

- Investigating breaches and recommending remedial actions.
- Organizing annual maintaining tests.

Estates Security

Responsible for:

- Physical security on company's estate.
- Administration of door access control systems
- Security of communication rooms and onsite data center.

Information Security Advisory Board

Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Human Resources

Human Resources is responsible for :

- Providing timely information regarding new Employees and termination of modification of employment status to managers and system administrator
- Providing a list of terminated employees for the purpose of auditing system accounts

System Users

All users of electronic resources and systems are accountable for any activity on the system performed with the use of their accounts.

Access control Policy

General identities

Generic IDs will not be normally permitted as means of access to Chattr data, but may be granted under exceptional circumstances if sufficient other controls on access are in place. Under all circumstances, users of accounts *must* be identifiable in order for Chattr to meet the conditions of its Internet Service Provider. Generic identities will *never* be used to access Confidential or sensitive data.

High-Level accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default. Authorization for the use of such accounts shall only be provided explicitly, upon written request from a senior manager (such as a head of department/division, or a departmental or center manager), and will be documented by the system owner. Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity (such as may happen via Ransom ware attacks, which typically are able to encrypt user data after

silently installing on a machine over which the user has admin privileges, or the creation of further user accounts).

Low-Level accounts

Access rights will be accorded following the principles of least privilege *and* need to know.

Maintaining data security levels

Every user should understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their sensitivity. The Information Classification Standard enables users to classify data appropriately and gives guidance on how to store it. Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security Policy and any other contractual obligations they may have to meet.

Access Control Authorization

User accounts

Access to Chattr resources and services will be given by having of a unique user account and complex password.

Staff User Accounts

Staff user accounts can only be requested in writing, and by using the appropriate forms, by departmental managers. No access to any Chattr staff IT resources and services will be provided without prior authentication and authorization of a user's account. By default, staff are provided with access to his/her space (with access denied to all other users), and an email account. They have access to a standard suite of software applications. By default, staff accounts will expire upon termination of contract, unless a request for an extension is received from the relevant Departmental Manager.

External Contractors

External contractors will be provided access through the External contractors Access Framework. By default, this service provides *no access to Chattr systems*. Only systems explicitly connected to the service by I will be able to use it.

Third parties

Third parties are provided with accounts that solely provide access to the systems and or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required.

Access for remote users

Access for remote users shall be subject to authorization and be provided in accordance with the *Remote Access Policy* and the *Information Security Policy*. No uncontrolled external access shall be permitted to any network device or networked system.

Passwords

Password issuing, strength requirements, changing and control will be managed through formal processes. The IT Service Desk for staff will manage password issuing. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects. Password changing can be performed on Chattr workstations, via LFY or the remote desktop. The system will enforce such requirements on their employees in in order to maintain the security of data such as:

- Passwords Must Meet Complexity Requirements such as : number of character , can't contain the user first or last name ,symbols ,numbers ,upper and lower case letters …etc.
- Enforce Password History in which the system won't allow the user to use old passwords or commonly used passwords.
- Maximum password Age in which the system enforces the user to change their password at least every three months and send different remainders to do so.
- Maintain password privacy by giving the users rules in which the are prohibited from sharing or uploading their passwords any where in which it can take advantage of.

Review and Development

This policy should be reviewed and updated regularly by the Information Security Advisory Board to ensure that it remains appropriate in the light of any relevant changes to the law, organizational policies or contractual obligations. Additional regulations may be created to cover specific areas. Information Security Advisory Board comprises representatives from all relevant parts of the organization. It should oversee the creation of information security policies. The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

Revision

The policy will be reviewed annually or when needed. Reviews will be published online and notified via emails.

REVISION HISTORY

Status	Published
Last Reviewed	02/29/2016
Last Updated	02/28/2015
Published	02/28/2015