CHATTR

Instant Messaging Policy

Overview

Instant Messaging as a tool for communication has seen a sharp rise in recent times due to its ease of use. The use of Instant Messaging tools in business seems desirable as they allow employees to interact with each other conveniently without relying heavily on emails and phone calls. They also allow employees to have group conversations from their desks. The asynchronous communication model and inability to see the person with whom you are conversing opens the door for many security threats and as such caution needs to be exercised while using IM tools.

Purpose

This document lists the usage policies for ChattrIM which should be followed to minimize the security incidents associated with IM tools.

Authorized Users

- The policy applies to all employees and contractors who have been provided with Chattr login credentials.

Usage Policy

- Users should use their Chattr email address to create a ChattrIM account.
- A strong password needs to be selected consistent with the password policy at ChattrIM. Refer Chattr Password Policy.
- Users must only add people from within the organization as contacts in ChattrIM.
- Users must always turn on automatic updates for ChattrIM. This allows latest security patches to be installed on your device.
- Any attachment downloaded via the IM must always be scanned before opening it. In case if any attachment is flagged by the antivirus, report it to InfoSec@Chattr.com .
- ChattrIM can be used remotely but only from a Chattr computer system.
- Users are allowed to engage in unofficial discussions. These conversations should be respectful and should maintain the same etiquette which users exercise while talking to fellow employees in person. (No slurs, inappropriate comments on color, race , gender will be tolerated).
- Always ensure to logoff from ChattrIM from multi-access terminals.
- Always ensure your computer is locked/shutdown when you are stepping aside.

Prohibited Use

- Users must use only ChattrIM for all instant messaging conversations. They should not install any 3rd party tools for IM conversations.
- Users should not share their login details with others.

- Users are prohibited from discussing highly sensitive information over ChattrIM.
- Users should not accept connection requests from individuals outside the Chattr Organization. It is advisable to send requests only to employees you have met in person.
- Users should not allow other Chattr employees and staff to use their ChattrIM account.
- Users should not use the system pretending to be someone else.
- Users should not accept or open attachments from unknown sources. Users should not open attachments that are flagged by the company's anti-virus software.
- Users should not send hyperlinks via the IM. Users should not open links sent to them on IM.
- Do not set your ChattrIM to automatically accept file transfers. Doing so increases the risk of downloading infected files.

Systems Management

Responsibilities

Information Security Team

- The InfoSec team should ensure users get updates for any security patches required for ChattrIM. Updates must be made available to users via Chattr Software Manager.
- The InfoSec team should ensure users have latest version of the antivirus running on their systems.

Users

- Users are expected to conduct themselves in accordance with professional standards, company's policy and law. The user should assume all legal liability that may result from inappropriate use of IM tools.

Security Governance Team

- All the data will be monitored by the security governance team for maintaining security. Any violations discovered will be actionable.

Violation of Policy

- All IM activities are subject to monitor and may be logged.
- Any violation of this policy will lead to disciplinary action which may lead to termination of employment.
- If you observe someone misusing the policy, report the same to InfoSec@Chattr.com

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