INFORMATION SECURITY MANAGEMENT SYSTEM

Acceptable Usage Standard

Version 1.8

Document Statistics

Type Of Information	Document Data
Document Title	Acceptable Usage Standard
Date of Release	09 Sep 2024
Document ID	ISMS_8.2_STD_PRC
Document Version No	1.8
Document Owner	Cyber Security Risk & Compliance
Security Classification	Internal
Document Status	Active

Document Revision History

Ver. No.	Date	Change Description	Author
1.0	05 Dec 2016	First Release	Mounika M – Audits & Compliance
1.1	26 Jul 2017	Annual Review ● Updated Section 5	Mounika M – Audits & Compliance
1.2	29 Jun 2018	Annual Review ● Updated section 5.6	Mounika M – Audits & Compliance
1.3	2 July 2019	Annual review	Mounika M – Audits & Compliance
1.4	10 Aug 2020	Annual review	Sai Sekhar P – Risk & Compliance
1.5	07 Aug 2021	Annual Review	Jeevana Pravallika P – Risk & Compliance
1.6	24 Jul 2022	Annual Review	Amba Bhavani P – Risk & Compliance
1.7	18 Jul 2023	Annual Review	Amba Bhavani P – Risk & Compliance
1.8	03 Jun 2024	Annual Review	Shravan Reddy – Risk & Compliance

Ver. No.	Reviewed By	Review Date	Approved By	Approved Date
1.0	Sridhar V - ISM	05 Dec 2016	Nishikant P – Compliance Head	05 Dec 2016
1.1	Raju I - ISM	3 Aug 2017	Nishikant P – Compliance Head	8 Aug 2017
1.2	Raju I - ISM	12 Jul 2018	Nishikant P – Compliance Head	13 Jul 2018
1.3	Raju I - ISM	09 Jul 2019	Nishikant P – Compliance Head	09 Jul 2019
1.4	Raju I – Director Risk & Compliance	17 Aug 2020	Ravi H – CISO	24 Aug 2020
1.5	Sairam Datla - ISM	20 Aug 2021	Raju I – Director Risk & Compliance	01 Sept 2021

1.6	Raju I – Director Risk & Compliance & Vartika Saxena - VP, Cyber Security	02 Aug 2022	Dane Jones - CISO	30 Aug 2022
1.7	Vartika Saxena - VP, Cyber Security	18 Aug 2023	Dane Jones - CISO	18 Sep 2023
1.8	Pushpendra Yadav - Manager Risk & Compliance	06 Sep 2024	Vartika Saxena - VP, Cyber Security	09 Sep 2024

Document Reference List

S. No.	Document Name
1	HighRadius_ISMS_POL_A8 Asset Management Policy v1.8
2	HighRadius_ISMS_STD_Disciplinary Standard v1.8
3	HighRadius_ISMS_PRC_Access Control Procedure v2.3

REVIEW

This document shall be reviewed once a year or at the time of any major change in the existing environment affecting policies and procedures, whichever is earlier.

For additional information, please contact

Corporate Headquarters:

HIGHRADIUS CORPORATION
2107 CITYWEST BOULEVARD
SUITE 1100
HOUSTON, TEXAS 77042
PHONE: (281) 968-4473
FAX: (281) 404-9002

Cyber Security: infosec@highradius.com
Privacy: privacy@highradius.com

Table of Contents

Acceptable Usage Standard

1. Introduction

The Acceptable Usage standard outlines the rules of thumb for the use and sharing of the information and computing facilities located at or used by HighRadius interns, employees, third-party service providers, and contractors. The standard consists of Do's and Don'ts which are required to be adhered to by all the intended users.

2. Objective

HighRadius Corporation provides employees with access to several resources to enable its employees to perform their job functions efficiently. These resources come as a privilege and with certain responsibilities. The Acceptable Use Policy defines these resources and their acceptable use.

3. Glossary

Abbreviation	Description
GM	General Manager
IMS	Infrastructure Management Services
CST	Cyber Security Team
ISMS	Information Security Management System
VPN	Virtual Private Network

4. Scope

The document outlines the rules for appropriate usage of the information and assets of HighRadius, and to apply appropriate protection mechanisms to ensure confidentiality, integrity, and availability of the asset. This policy applies to all employees, Interns, partners, third-party service providers, and contractors who have access to HighRadius' information systems.

5. General Use and Ownership

- Users are required to use and manage Highradius computing resources responsibly, in a way that maintains the confidentiality, integrity, and availability of its information assets.
- Users are responsible for protecting any information stored on their Highradius assets.
- Preventing the misuse of the assigned Access Card / Visitor Card is the responsibility of the cardholder.
- Employees should not leave printed/faxed documents at the printers/fax machines unattended.
- Employees are authorized to print documents and/or data only for valid business purposes.
- Users shall cooperate and support the activities such as fire drills and maintain security compliance at all times.

- Users should ensure that their laptops and application OS patches are up to date by connecting to the Highradius network or VPN accordingly or restarting their machines when the auto-updates prompt for.
- Users will not be allowed to update the machines, wherein the IT team will push the updates from a central service and users should restart their machines when prompted for.
- Any anomalies noted in systems and networks (e.g., suspicion of virus attacks, malicious code, loss or compromise of passwords, theft of equipment like hard disks, laptops, blackberry, portable storage devices, etc.) shall be promptly reported to the security incident e-mail id infoSec@highradius.com. or Genie tickets under: Cybersecurity Desk > Security Issues > Security Incidents
- For physical loss or theft of assets, the Admin & facility team should be notified simultaneously by sending an email to admin@highradius.com or by reaching out through appropriate communication channels. This communication has to flow from either the affected user or the user's line manager
- Use of the Internet and e-mail should be only for business-related information exchange and limited personal use of HighRadius systems is acceptable as long as it does not violate HighRadius data leakage policies.
- Users are expected to read thoroughly and abide by the Password Guidelines as mentioned in the Password Standard (Password Management Procedure). as the guidelines are mentioned in the **HighRadius_ISMS_PRC_Access Control Procedure**.
- If any additional software is required by a user, it shall be installed and configured by authorized (IMS) personnel, after approval from Cyber Security. HighRadius can at any time remove/uninstall such software from the infrastructure or workstations if the requirement is no longer justified for business or it is noticed that it is not needed for business.
- Removable media should be disabled by default on all systems and for any exceptions required, the user needs to raise a Genie Ticket on 'Cybersecurity desk' and an approval should be obtained from the VP - Cyber Security/GM prior to providing any such access.
- Employees are not authorized to connect any personal device to the company network for data transfer and device charging.
- Before leaving the workstation, the user must, at all times, log off or lock the workstation
- Employees should clear their workstations/ desks before leaving for meetings, lunch, or at the end of the day. Cabinets should be locked when not in use.
- Users shall not make copies of system configuration files for their own, personal use or to provide to other people/users for unauthorized uses.
- Before termination of employment, the employee should make relevant business information accessible to their reporting manager.
- Users, if using smartphones/tablets for accessing corporate emails, should ensure that password protection or any other means of authentication is enabled on the smartphone/tablet. Installation of Antivirus programs is advisable to ensure protection from viruses /malware etc.
- Users must not place any HighRadius restricted/internal/confidential/highly confidential information in a publicly accessible Internet site that supports FTP or similar services without prior approval.

- Users are responsible for protecting any information used and/or stored in their HighRadius accounts.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code or have extensions like exe, bat, drv, vxd, etc.
- Periodic awareness and training on Information Security shall be conducted to facilitate user understanding and compliance to the policies, procedures, and standards. It is mandatory for each user to participate in/attend the training at least once every year.
- The data on HighRadius' network shall be the property of HighRadius and any unauthorized access, copying, modification, or destruction of the data is prohibited.
- For any exceptions to the above-mentioned point explicit Highradius management approval is required in conjunction with one's professional roles and responsibilities.

5.1. PCs, laptops, and workstations

HighRadius-issued PCs, laptops and workstations

- Laptops must not be left unattended at any point in time, when not in HighRadius premises or at the user's home.;
- Laptops must be securely stored when not in use;
- Users shall save all important documents on the respective HighRadius cloud storage to ensure that work isn't lost if a laptop is lost or stolen or a disk failure;
- Users must not keep their laptops in 'Hibernate' mode. They must be properly closed down (i.e., selecting shutdown from the operating system menu) when not in use and secured in a suitable locked cabinet within their place of work;
- Any user who steps away from the workstation for any period of time must ensure that it is left 'locked'. (By pressing 'ctrl + alt + del' and choosing 'lock this computer or pressing the windows key and 'L')';
- Only approved users with administrator privileges on their PCs will be allowed to –
    - Reinstall Licenses/ approved Software application for troubleshooting purposes
    - Execute Licensed/ approved Software application that doesn't run without Admin Privilege
    - The same must be requested by raising a request in the ticketing portal with approval from Line manager and Cyber Security Manager;
- Damage to (including suspected tampering) or loss of the laptop must be reported to the Administration or IT Helpdesk team who will advise on the action that must be taken;
- User shall not attempt to disable/alter the software/configuration of PCs/Laptops;
- HighRadius authorized personnel shall have unrestricted access to the PCs/Laptops for investigation/support purposes;
- End Users should not take photographs, video, and audio recordings to capture any client information and HighRadius Restricted/Confidential information.

5.2. Passwords Management

Users shall follow HighRadius' Password Management and Secure log-on Standard for composing strong passwords; Please refer to the complete password standards from **HighRadius_ISMS_PRC_Access Control Procedure**

5.3. Internet

Users shall not attempt to use or allow HighRadius' Internet Service to be used to:

- Engage in any activity that is illegal under local, state, or international law;
- Access or download unauthorized and non-business-related software, including games, games upgrades or related software;
- Download, transmit, view or store material which could be considered as pornographic, vulgar or profane; insulting, defamatory or offensive to any individual/community/ religion or organization; and which could harm HighRadius' status or reputation;
- Use unapproved chat software (e.g.; Skype for Personal, lRC, MIRC, yahoo, messenger, MSN messenger, etc.). Prior approval must be obtained from Business Group Head of the requesting user (s) and the VP - Cyber Security/GM for use of any unapproved chat software, in case of any business requirement;
- Conduct an act of electronic harassment of any kind;
- Store, send or distribute sensitive or confidential information, copyrighted material, or other content which is subject to HighRadius or third-party intellectual property rights;
- Tamper with, hinder the operation of or make unauthorized modifications to any network or system;
- Send or distribute unsolicited advertising, bulk electronic messages or overload any network or system;
- Access, monitor or use any data, systems or networks, including another person's private information, without authority or attempt to probe, scan or test the vulnerability of any data, system or network;
- Obtaining unauthorized access to or knowingly modifying information held on Internet resources;
- Access to the Internet from HighRadius' computers has been provided as a business resource. Inappropriate personal use will be treated as a disciplinary offense. HighRadius reserves the right to monitor Internet traffic to prevent any activity that may be illegal, unauthorized, or harmful to the Company, its employees/contractors, clients, or business partners. HighRadius also retains the right to block access to any Internet website/category of websites/online serves as it deems appropriate.

5.4. Wi-Fi

- Users shall not use HighRadius' Wi-Fi in a way that violates the law or the established processes/ policies of HighRadius;
- HighRadius Wi-Fi connection is for official use only. Users shall not use Wi-Fi for any commercial purpose;

- Users shall not attempt to deceive others about their identity in electronic communications or another network traffic;
- Users shall not use Wi-Fi connection to threaten, intimidate, or harass other individuals;
- Usage of unsecured and open wireless networks is prohibited for Highradius systems
- If Wi-Fi connection of a user sends disruptive signals, or violates any of the above requirements, it will constitute a violation of HighRadius' Regulations and could result in administrative or disciplinary procedures; and
- The Wi-Fi network connection may be subject to monitoring, with cause, for security, legal, or troubleshooting purposes. This may include monitoring for bandwidth usage, security-related incidents, or a request from legal/law enforcement authorities. In addition, the Risk & Compliance team reserves the right to scan the network to assist in identifying and protecting against exploitable security vulnerabilities (e.g., viruses or worms) in efforts to preserve network integrity. Information gathered in such scans will be used only for the explicit purpose of monitoring network security.

5.5. Usage of VPN

- Users with remote access privileges shall directly access only those services that they are specifically authorized to use;
- Only VPN client software distributed by HighRadius must be used to connect to the HighRadius VPN. Approved users can download the VPN client and installation instructions from HighRadius;VPN is installed on all the corporate laptops by default.
- User is responsible for any activity performed using his/her account;
- Peer-to-peer software is not allowed in HighRadius Network directly or over VPN connection.
- Anti-Virus software is also installed by default by IT Team in all the corporate laptops and patches are also managed via centralized tool, hence we might either modify the point or remove.
- It is the responsibility of the user with VPN privilege to ensure that unauthorized users are not allowed access to the HighRadius network;
- Users shall not use the VPN for web surfing that does not otherwise require it for access. In other words, when the user has completed accessing the HighRadius Intranet, they must end the VPN session before normal web access;
- HighRadius Risk & Compliance team reserves the right to audit all VPN client systems and all communication between VPN client systems and the HighRadius network for compliance with all applicable Information technology Services security requirements; and

To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified and resolved. Any HighRadius employee found to have intentionally violated the VPN Acceptable Use will be subject to disciplinary action.

5.6. Network and system activities

The following activities are strictly prohibited, with no exceptions:

- Port scanning or security scanning unless prior permission is sought from Cyber Security Team or required as part of employees' normal job duty;
- User shall not attempt to connect to any server/Network element that they do not have authority to access or needed to carry out their job functions;
- Executing any form of network monitoring which will intercept data not intended for the employee's or contractor's host, unless this activity is a part of the employee's / contractor's normal job/duty;
- Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to, accessing data of which the employee/ contractor/ third party user is not an intended recipient or logging into a server or account that the employee/ contractor is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
- Revealing account password to others or allowing the use of the account by others. This includes family and other household members when working from home;
- Making copies of system configuration files for users' own, unauthorized personal use or to provide to other people/users for unauthorized use;
- Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session via any means locally or via the Internet/intranet/Extranet unless this activity is a part of the employee's normal job duty;
- Circumventing user authentication or security of any host, network or account;
- Downloading, installing or running security programs or utilities which reveal weaknesses in the security of a system.
- Disabling any security tools (such as AV/ EDR/ CASB/ DLP) from user workstations or servers without prior consent and approval from the Cyber Security team.
- Only authorized users from Internal IMS are permitted to temporarily uninstall any aforementioned security tools from a user workstation, solely for the purpose of any troubleshooting. Any such uninstallations should be informed to the Cyber Security team promptly. Further, once the issue is resolved, the tool should be installed back on the user workstation.
- Users with administrator privileges on their PCs will not be allowed to –
  - Reset the local Administrator account password;
  - Uninstall existing HighRadius IT installed software;
  - Uninstall/disable Antivirus software or other security tools such as DLP, CASB, EDR, etc.;
  - Disable Windows Firewall;
  - Create/modify/remove any user accounts
  - Sharing the folder with all domain user permissions.

5.7. Email

General Requirements for all employees

- All messages generated by email shall be considered to be the property of HighRadius;
- Users shall safeguard their email account by creating strong passwords as per HighRadius' password policy. Users should not disclose their password to anyone else under any circumstances;
- The following activities are strictly prohibited:
  - Sending implied or explicit messages which criticize other individuals or organizations;
  - Sending or forwarding emails containing defamatory, offensive, or obscene expressions;
  - Postings by employees from HighRadius email address to any newsgroups, unless posting is in the course of business duties;
  - Making fraudulent offers of products, items, or services;
  - Any form of harassment via email, whether through language, frequency, or size of messages;
  - Unauthorized use, or forging, of email header information;
  - Creating or forwarding "chain mails"; and
  - Knowingly distributing files that contain viruses, spyware, Trojan horses, worms, logic bombs, cancelbots, corrupted files, rootkits or any other similar software or programs that may damage the operation of another's computer, network system or other property.
  - Access to Non -highradius email accounts is prohibited,
  - Users should not open e-mails or attached files without ensuring that the content appears genuine. If not expected to receive the message or are not certain about its source, do not open it and report the same to CyberSec via PhishRIP.
  - Employees should understand that HighRadius will have access to all information stored or transmitted through HighRadius computers and/or networks, including employee personal information. Therefore, employees should have no expectation of privacy as the information they voluntarily place on these computers and/or networks.

Archiving

- Archiving of sent and received emails shall be performed by the Email Administrator based on defined schedules;
- Emails shall be archived as per the legal requirement based on the technical feasibility of the archiving solution;
- End users are not allowed to administer their mail in the archive system; and
- Archive Admin activity log must be recorded.

SPAM Mails

Users shall not use or allow their email/ internet service to be used for:

- Sending multiple unsolicited electronic mail messages or "mail-bombing" - to one or more recipients ;
- Sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
- Using redirect links in the unsolicited commercial e-mail to advertise a website or service;
- Using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients to conduct any of the prohibited activities under this Standard;
- Falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- Using or distribute any software designed to harvest email addresses;
- Hosting any device or service that allows email to be sent between third parties not under HighRadius authority or control.
- Users can reduce the amount of Spam by following the below-mentioned practices:
    - Use separate email addresses for different purposes, such as a personal email address for friends and family and a business email address for work;
    - Do not open emails from dubious sources;
    - Do not reply to Spam or click on links, including ‘unsubscribe' facilities, in Spam;
    - Do not accept Spam-advertised offers;
    - Do not post your email address on publicly available sites or directories. If you must do so, look for options, such as tick boxes, that allow you to opt out of receiving further offers or information.;
    - Do not disclose your personal information to any online organization unless they agree (in their terms and conditions or privacy policy) not to pass your information on toies;
    - Report any Spam you receive to the Cyber Security Team.

5.8. Usage of personal information

- Users are expected to respect the privacy of others. Any attempt to gain an unauthorized access to private information or passwords (via technological or social means) is prohibited. Any form of identity theft or the compromising of another individual’s personal information is a violation of the privacy and is subject to disciplinary action.
- Users in the custody of personal information of employees/clients shall not disclose the same to a third party except if agreed through contractual agreements for business purposes. If HighRadius consigns the handling of personal data to a subcontractor, HighRadius will select an entity that is deemed as handling personal data appropriately and manage the contracted entity as necessarily and appropriately so that entrusted data is under safe control;
- Employees shall not remove records containing personal information from the office unless it is necessary for carrying out their job duties, post required approvals;
- Paper records containing personal information should be securely packaged in folders to protect against disclosure/ theft;

- Personal information should never be viewed on a laptop screen while traveling on public transportations;
- Employees are prohibited from sending personal information by e-mail or fax unless it is necessary to do so for business purposes; and
- Any breach of privacy or loss or theft of personal information should be reported immediately to the Privacy (privacy@highradius.com) Network Security and Cyber security Team, who may launch an investigation, if necessary.

5.9. Copyright infringement

- HighRadius supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement;
- Users shall not use HighRadius' resources to copy, adapt, reproduce, distribute, or otherwise make available to other persons any content or material (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text, and downloaded information) which is subject to copyright or do any other acts with this copyright material which would infringe the exclusive rights of the copyright owner or any applicable law;
- Users shall not transmit, distribute, download, copy, cache, host, or otherwise store any information, data, material, or work that infringes the intellectual property rights of others; and
- Installation of unlicensed software or unauthorized web extensions is strictly prohibited. Disciplinary action shall be taken if unlicensed software is found on PC/laptop assigned to the user.

5.10. Software usage

Restriction on installation

- HighRadius will provide copies of legally acquired software to meet all legitimate needs in a timely fashion and in sufficient quantities for all of its computers. The use of software obtained from any other source could present security and legal threats to the company, and such use is strictly prohibited;
- Software must be selected from an approved software list, maintained by the Internal IMS Team unless no selection on the list meets the requester's need.
- End users shall be prohibited from installing any new software or hardware on any HighRadius device, including desktop computers, servers, or portable computers, without prior approval. All new software, not covered under the authorized software list must be approved by the Cyber Security team before installation on information systems; any such software should be procured through IMS as a licensed version and cyber would perform security testing on it before deployment.
- Software requests must first be approved by the requester's Line Manager and the Cyber Security Team, and then be routed to the IT Helpdesk to be implemented by Internal IMS;
- IMS team shall maintain the current list of approved software inventory and ensure the list is available to all the user's.

Privileged utility programs

- Access to system utilities should be granted only to privileged users who are authorized and have a business case for accessing the specific system utility. If the utility supports different privilege levels, it should be ensured that the privilege level is set based on the need-to-know/ need-to-do basis;
- The system utilities should be kept separate from other normal user utilities/ programs. At any point, a normal user should not be able to gain access to any of the system utilities, without prior approvals;
- All default system utilities that are considered unnecessary, if installed during the commissioning of a new information system should be deleted/ uninstalled during the deployment process;
- Many equipment/ applications are provided with diagnostic ports for remote diagnostic/ maintenance tasks through system utilities. Access to such ports should be restricted only to authorized sources and reviewed on a periodic basis;
- If the system utilities are used for remote administration/ maintenance tasks, remote access should be limited from pre-defined IP / Host addresses.; and
- All changes and activities performed by privileged users using system utility need to be logged and monitored.

Duplication of licenses

- Software shall not be duplicated, reproduced, or installed on more than one machine without the prior written authorization of the IMS Team;
- If a software license states it is eligible and approved for multiple uses, the following conditions must be adhered to:
  - Use of the software is limited to HighRadius business; and
  - The software must be removed from the computer if the individual is no longer employed by HighRadius.

Monitoring

- Cybersecurity Team reserves the right to decline any software request that:
  - Causes conflicts with currently installed software
  - Poses security risks
- HighRadius has the authority to uninstall any unauthorized software or hardware if it is discovered
- HighRadius reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorized copies of software. These controls may include periodic assessments of software use, announced and unannounced audits of company computers to assure compliance and the removal of any software found on HighRadius' property for which a valid license or proof of license cannot be determined, and any disciplinary actions required on the basis of the findings.

6. Unacceptable Use

6.1. Network and System Activities

The following activities are prohibited and are determined as unacceptable:

- Use or attempts to use resources without authorization is strictly forbidden. This includes unauthorized access to, manipulation, and distribution of information.
- Users shall not share login credentials/passwords of their systems with anyone, for any purpose.
- Users shall not use Intellectual Property, including copyrighted material, trademarks, and trade secrets of other organizations or entities without appropriate management approval.
- Processing and/or storage of HighRadius information on IT resources which are not owned or controlled by HighRadius, is not permitted without written approval from the relevant business owner.
- Unless explicitly authorized, testing, experimenting, or exploiting weaknesses of the HighRadius network shall be treated as a policy violation and may result in disciplinary action.
- Users shall not spread viruses and malicious code into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

6.2. Email and communication activities

The following activities are prohibited and are determined as unacceptable:

- Users shall not send unsolicited email messages, pornographic images, defame or impersonate content, or engage in any form of harassment via email, telephone, or paging.
- Automatic forwarding of emails to external addresses is not permitted without appropriate approval.
- Any personal e-mail communication outside the HighRadius network shall not contain any information which connects it to HighRadius or gives the impression that personal opinion is directly/ indirectly HighRadius opinion.
- HighRadius e-mail address shall not be used for private subscriptions and mailing lists. Users shall not use HighRadius e-mail to spam other email users or newsgroups.
- Users shall not change any information embedded into the e-mail such as the header, date, time, or other information unless authorized to do so.
- Employees shall not employ any electronic mail addresses other than official company electronic mail addresses for all company business matters.
- Only authorized personnel specifically delegated and approved by the department heads and human resources can monitor electronic mail systems.

6.3. Internet Usage

The following activities are strictly prohibited, with no exceptions:

- Access to the Internet from HighRadius computing devices has been provided as a business resource. Excessive or inappropriate personal use will attract disciplinary action.
- HighRadius reserves the right to monitor Internet traffic for the purpose of preventing any activity that may be illegal, unauthorized, or harmful to the Company, its employees/contractors, clients, or business partners
- HighRadius retains the right to block access to any Internet website
- Obtaining unauthorized access to or knowingly modifying information held on Internet resources
- Transmitting any HighRadius computer/user id or password information unless it's for a business need.

7. Violation of Standard and Consequences

Following activities, but not limited to, constitute security violations:

- Non-compliance with the requirements of HighRadius Information Security Policy and associated standards or procedures;
- Exposing HighRadius to actual or potential monetary loss through the compromise of security;
- Disclosure of confidential information or unauthorized use of the HighRadius information and information processing facilities;
- Usage of hardware, software or information for unauthorized or illicit purposes which may include violation of any law, regulation or reporting requirements of any law enforcement or government body.
- Violations of the rights of any person or company protected by privacy, copyright, trade secret, patent, or other intellectual property, or similar laws or regulations.

Any conduct of these activities can be treated as gross misconduct and imply disciplinary action for the individual(s) involved as per the *HighRadius - Disciplinary Action*

Users should promptly bring any such breach to the notice of the *Line Manager / Security Incident mail ID* infosec@highradius.com or Genie tickets under: Cybersecurity Desk > Security Issues > Security Incidents. Also, in case of breach or violation;

- HighRadius, through authorized personnel, has the right to audit or access all information stored on HighRadius IT resources, regardless of ownership, location of storage, or labeling, with or without prior notice.

- All activities within HighRadius computing resources can be traced back to individual users. All HighRadius resources can be monitored and all authorized as well as attempts at unauthorized use can be logged.