INSTANT IT TECHNOLOGY

IT Security Policy

IT Acceptable Use Policy

Title of work:	INSTANT IT TECHNOLOGY/InfoSec	Year of Creation of Work:	2023
Category:	Internal	Full Date of Publication:	01-Aug-23
Version:	V0.1	Total Pages:	33
Description:	This document provides details about Acceptable Usage policy & guidelines	Reviewed by:	Legal & IT
Author:	IT Compliance	Approved by:	Head - IT - Operation & BD Team

This internal document is the property of **INSTANT IT TECHNOLOGY.** & Creator Author. All use, disclosure, distribution, and/or reproduction not specifically authorized by HO IT & Compliance Dept of **INSTANT IT TECHNOLOGY.**, are prohibited. The information contained in this document is proprietary & internal and is intended for use only by the person to whom it is specifically issued in the first place. This document is not to be loaned to anyone, within or outside the organization. Copying or distribution of this document without consent of HO IT & Compliance Dept is unauthorized and illegal. If this volume is lost or stolen, the holder must immediately notify HO IT & Compliance Dept of **INSTANT IT TECHNOLOGY.,** If found, please return to HO IT & Compliance Dept of **INSTANT IT TECHNOLOGY.,** please contact IT compliance Office of **INSTANT IT TECHNOLOGY.**, for clarifications, comments, and suggestions with respect to any matter in this document.

INFORMATION SECURITY POLICIES

Acceptable Use Policy

1.0 Overview

This policy protects RESPL' employees and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of RESPL These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every RESPL Employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at RESPL These rules are in place to protect the employee and RESPL Inappropriate use exposes RESPL to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at RESPL including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by RESPL.

4.0 Policy

4.1 General Use and Ownership

1. While RESPL'S network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of RESPL Because of the need to protect RESPL'S network, management cannot guarantee the confidentiality of information stored on any network device belonging to RESPL.

2.RESPL recommends that any information that users consider sensitive or vulnerable be encrypted by the software provided by RESPL.

3.For security and network maintenance purposes, authorized individuals within RESPL may monitor equipment, systems and network traffic at any time.

4. RESPL reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1.Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed every month. Passwords should contain at least 8 characters.

2.All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging- off when the host will be unattended.

3. Use encryption of information in compliance with RESPL'S Acceptable Encryption standard.

4. Because information contained on portable computers is especially vulnerable, special care should be exercised.

5.Postings by employees from an RESPL, email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of RESPL unless posting is in the course of business duties.

6.All hosts used by the employee that are connected to the RESPL LAN/Internet/Intranet/Extranet, whether owned by the employee or RESPL, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

7.Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of RESPL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing RESPL. Owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited with no exceptions:

1.Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by RESPL.

2.Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which RESPL or the end user does not have an active license is strictly prohibited.

3.Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.

5.Revealing your account password to others or allowing use of your account by others.This includes family and other household members when work is being done at home.

6.Using a RESPL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any RESPL account.

8.Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. 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.

9.Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

10. Circumventing user authentication or security of any host, network or account.

11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

12.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.

13. Providing information about or lists of RESPL employees to parties outside RESPL.

Email and Communications Activities

1.Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use or forging of email header information.

4.Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6.Use of unsolicited email originating from within RESPL'S networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by RESPL or connected via RESPL'S network.

7. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

4.4. Blogging

1.Blogging by employees, whether using RESPL'S property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of RESPL'S systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate RESPL'S policy, is not detrimental to RESPL'S best interests, and does not interfere with an employee's regular work duties. Blogging from RESPL'S systems is also subject to monitoring.

2.RESPL'S Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any RESPL confidential or proprietary information, trade secrets or any other material covered by RESPL'S Confidential Information policy when engaged in blogging.

3.Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of RESPL and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by RESPL'S Non- Discrimination and Anti-Harassment policy.

4.Employees may also not attribute personal statements, opinions or beliefs to RESPL when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of RESPL Employees assume any and all risk associated with blogging.

5.Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, RESPL'S trademarks, logos and any other RESPL. Intellectual property may also not be used in connection with any blogging activity.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

PASSWORD POLICY

1.0 Overview Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of RESPL'S entire corporate network. As such, all RESPL employees (including contractors and vendors with access to RESPL systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any RESPL facility has access to the RESPL network, or stores any non-public RESPL information.

4.0 **Policy**

4.1 General

· All passwords (e.g., Administrator, root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.

· All production system-level passwords must be part of the RESPL administered global password management database.

· User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

· Passwords must not be inserted into email messages or other forms of electronic communication.

· All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at RESPL Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voice mail password, and local router logins.

Poor, weak passwords have the following characteristics:

- The password contains less than 6 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Name of family, pets, friends, co-workers, fantasy characters etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words “RESPL”, “India”, “Sanfran”. or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word of number patterns like aaabbb, QWERTY, zyxwvuts, 123321, etc.
    - Any of the Above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have Digit and Special characters as well as letters e.g., 0,9, !@#$%^&*()_+\~-=\`{}[]:”;’<>?,./)
- Are at least 6 alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Is not a word in any language, slang, dialect, jargon, etc?
- Are not based on personal information, names of family etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for RESPL accounts as for other non-RESPL access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various RESPL access needs.
Do not share RESPL passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive, Confidential RESPL information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., “my family name”)
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every one month (except system-level passwords which must be changed required). The recommended change interval is every one month.

If an account or password is suspected to have been compromised, report the incident to RESPL and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by RESPL or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Use of Passwords and Passphrases for Remote Access Users

Access to the RESPL Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

INSTANT IT TECHNOLOGY EMAIL USE POLICY

1.0 Purpose To prevent tarnishing the public image of RESPL When email goes out from RESPL the general public will tend to view that message as an official policy statement from the RESPL.

2.0 Scope

This policy covers appropriate use of any email sent from an RESPL email address and applies to all employees, vendors, and agents operating on behalf of RESPL.

3.0 **Policy**

3.1 Prohibited Use. The RESPL email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any RESPL employee should report the matter to their supervisor immediately.

3.2 **Personal Use.**

Using a reasonable amount of RESPL resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from an RESPL email account is prohibited. Virus or other malware warnings and mass mailings from RESPL shall be approved by RESPL'S System/ Mail administrator before sending. These restrictions also apply to the forwarding of mail received by a RESPL employee.

3.3Monitoring

RESPL employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. RESPL may monitor messages without prior notice. RESPL is not obliged to monitor email messages.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

REMOVABLE MEDIA POLICY

1.0 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

2.0 Purpose

To minimize the risk of loss or exposure of sensitive information maintained by RESPL and to reduce the risk of acquiring malware infections on computers operated by RESPL.

3.0 Scope

This policy covers all computers and servers operating in RESPL.

4.0 Policy

RESPL staff may only use RESPL removable media in their work computers RESPL removable media may not be connected to or used in computers that are not owned or leased by the RESPL Without explicit permission by system administrator or management of the RESPL.

When sensitive information is stored on removable media, it must be encrypted in accordance with the RESPL Acceptable Encryption software.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

ANTI-VIRUS USER POLICY

1.0 Overview

Virus, Worms, Trojan horse, Spywares is a well-known source of malware infections and has been directly tied to the loss of confidentiality and integrity of sensitive information in organizations.

2.0 Purpose

To establish requirements which must be met by all computers connected to RESPL networks to ensure effective virus detection and prevention.

3.0 Scope

This policy applies to all RESPL computers that are PC-based or utilize PC-file Directory sharing. This includes, but is not limited to, desktop computers, laptop computers, FlLE/HTTP/MAIL/FTP/TFTP/SQL/proxy servers, and any PC based equipment.

4.0 Policy

All RESPL computers must have RESPL'S standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into RESPL'S networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

5.0 Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with RESPL Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- New viruses are discovered almost every day. This Recommended to update antivirus periodically.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

SERVER SECURITY POLICY

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by RESPL Effective implementation of this policy will minimize unauthorized access to RESPL proprietary information and technology.

2.0 Scope This policy applies to server equipment owned and/or operated by RESPL and to servers registered under any RESPL- owned internal network domain. This policy is specifically for equipment on the internal RESPL network. For secure configuration of equipment external to RESPL on the DMZ

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at RESPL must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by RESPL Operational groups should monitor configuration compliance and implement it tailored to their environment. Configuration changes for production servers must follow the appropriate change management procedures.

3.2 **General Configuration Guidelines**

- Operating System configuration should be in accordance with approved RESPL.
- Services and applications that will not be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

- Always use standard security principles of least required access to perform a function.
- Do not use Administrator when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3. Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - ❖ All security related logs will be kept online for a minimum of 1 week.
  - ❖ Daily incremental backups will be retained for at least 10 days.
  - ❖ Weekly full backups will be retained for at least 1 week.
- Security-related events will be reported to RESPL, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - ❖ Evidence of unauthorized access to privileged accounts
  - ❖ Anomalous occurrences that are not related to specific applications on the host.

4. Compliance

- Audits will be performed on a regular basis by authorized person within RESPL.
- Audits will be managed by the internal audit group or RESPL authorized person. In accordance with the *Audit Policy*. RESPL will filter findings not related to a specific Operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

USER ACCOUNT/EMAIL CREATION AND TERMINATION POLICY

1.0 Overview
User account names are just as important to computer security as passwords. Without unique user name accounts that can be associated with a single individual, auditing and access controls are difficult if not impossible. As such, all RESPL'S employees (including contractors and vendors with access to RESPL systems) who require accounts will have accounts assigned to them that conform to the guidelines below.

2.0 Purpose The purpose of this policy is to establish a process by which all user accounts are uniquely identifiable to the individual or process that uses them.

3.0 Scope The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at any RESPL facility, has access to the RESPL network, or stores any non- public RESPL information.

4.0 Policy
All user accounts are to be unique and each user account must never be used by another individual after creation. User account will remain with the individual throughout the entirety of their relationship with Over & Above Software & Infrastructure Solutions and will not be assigned to future employees, contractors and vendors in the event of termination of relationship. Any access required on the network by each individual will require the usage of this unique user account and the associated authentication methodology.

4.1 Single Sign-In
To assist in managing this process, single sign-on capabilities will be used wherever possible. This means that the account created for each user in the primary network operating system environment for RESPL will be used as the user account information for access to all third party applications whenever possible. In cases where this is not able to be done, this will be documented.

4.2 Username format

Accounts will be created using the standard

- If first name of employee or user is unique on centralized authentication server then the first name of employee or user is used for creating user name else
- The first name of employee/user followed by underscore (_) or dot (.) and then his/her last name is used for creating user name else
- The first name of employee/user followed by his/her at least first character of last name is used for creating user name

All user accounts will have the user's full name included with the account so they can be uniquely associated with the specific individual for which the account was created.

4.3 Request for creation and termination of account Request for creation and termination of account is only accepted from HR Department of RESPL Request is send in form of Email or in Hardcopy and must accompany valid proof of joining of the employee such as Employee Id generated from the Companies designated Software or any other documentary Evidence.

4.4 Termination of relationship Upon termination of relationship with RESPL, the accounts for the user will be disabled, but not deleted for one week. The account will be enabled and available with changed password to upper management of RESPL on their request.

4.5 Service Accounts

It is reasonable to anticipate that accounts will need to be created that are not uniquely associated with a specific user. These accounts are to be for special purposes, such as for running scheduled batch jobs, backups, service applications or like that. These accounts must be unique to the process or function for which they are intended.

5.0 Enforcement

The responsibility for complying with this policy belongs to the personnel responsible for creating accounts. Any employee found to have violated this policy may be subject to disciplinary action.

CONFIDENTIAL DATA SANITIZATION POLICY

1.0 Overview

RESPL'S employees often have a business need to store Confidential on their personal computers. Yet when it comes time to dispose of these systems, or transfer them to another user, there are few established policies and processes in place to prevent confidential data from being accessible by unauthorized persons.

2.0 Purpose The purpose of this policy is to present recommended policies and guidelines that describe the process by which confidential data may be permanently removed from a server, personal computer, and workstation, PDA or CD/DVD in such a way that the data is deliberately made no recoverable. In other words, this document discusses when and how to sanitize disks, devices that may be mounted as disks (e.g., flash memory devices) and other common data storage products.

3.0 Scope The scope of this policy is covers all servers, personal computers, Laptops, PDA and like devices used by RESPL'S employees. The devices discussed here include magnetic disks, flash memory devices, CDs and DVDs, and PDAs (Palm Pilots, Pocket PCs and Smart phones) and like devices. A device that has been sanitized has no usable residual data and even advanced forensic tools should not ever be able recover erased data. It is possible to sanitize a single file, a set of files, or an entire disk or device. Sanitization processes include using a software utility that completely erases the data.

4.0 Policies

In all cases, the device is assumed to contain confidential data.

4.1 Device transferred to a person who is not intended to see confidential data. When a computer is transferred from one person to someone who works in a different organizational unit, all confidential data on the system should be sanitized, either the confidential data files or the entire disk should be erased according to directions in the Sanitization Guidelines section.

4.2 Device to be disposed of or transferred off RESPL

When a computer is to be disposed off or transferred to someone not working for with RESPL, all disks should be sanitized, whether or not they are known to contain any confidential data. No disks, including flash memory devices, should be disposed of without being sanitized.

5.0 Data Sanitization Guidelines

The program/software that uses for data sanitization must use at least any one of the following algorithm

- Guttmann method: This is an algorithm for securely erasing the contents of computer hard drives, such as files. It does so by writing a series of 35 patterns over the erased region.

- US DoD 5220.22-M: US Department of Defense in the cleaning and sanitizing standard DoD 5220.22-M recommends the approach "Overwrite all addressable locations with a character, its complement, then a random character and verify"

A user can use any of the above mentioned algorithms; however RESPL recommends Guttmann method for secure deletion.

Computer Disk Sanitization and Destruction Disk sanitization involves securely erasing all the data from a disk so that the disk is, except for the previous wear, “new” and empty of any previous data. There is no way to use any operating system to effectively sanitize the same operating system disk. In other words, an operating system cannot securely erase the disk that it is “running off of”. However it is possible to use operating system commands to sanitize a nonoperating system disk.

CD and DVD Destruction CDs and DVDs that contain confidential data need to be physically destroyed when they are no longer needed. Paper shredders can often do this as can special CD/DVD destruction hardware

Note: If possible destroy the media physically. Physical destruction involves either taking apart the disk and cutting the platters into small pieces or otherwise destroying the disk (e.g., high temperature or crushing).

FIREWALL CONfiGURATION POLICY

1.0 Overview

Firewalls protect sites from exploitation of inherent in providing robust system security for large numbers of computers. There are several types of firewalls, ranging from boundary routers that can provide access control on Internet Protocol packets, to more powerful firewalls that can close more vulnerability in the TCP/IP protocol suite, to even more powerful firewalls that can filter on the content o the traffic.

2.0 Purpose

Firewalls are able to work in conjunction with tools such as intrusion detection monitors and email/web content scanners for viruses and harmful application code. But firewalls alone do not provide complete protection from Internet borne problems. As a result, they are just one part of a total information security program. Generally firewalls are viewed as the first line of defense, however it may be better to view them as the last line of defense for an organization; organizations should still make the security of their internal systems a high priority. Internal servers, personal computers, and other systems should be kept up-to-date with security patches and anti-virus software.

3.0 Scope This policy provides introductory information about firewalls and firewall policy primarily to assist those responsible for network security. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewall environments.

4.0 **Firewall policy** A firewall policy guides how the firewall should handle applications traffic such as web, email, or telnet. The policy should describe how the firewall is to be managed.

The steps involved in creating a firewall policy are as follows:

- Identification of network applications deemed necessary
- Identification of vulnerabilities associated with applications
- Creation of firewall rule set based on applications traffic

Firewall configuration guidelines

Most firewall platforms utilize rule sets as their mechanism for implementing security controls. The contents of these rule sets determine the actual functionality of a firewall.

Nearly all rule sets, however, will contain at least following fields:

- **Source Address of the packet,** the Layer 3 address of the computer system or device, the network packet originated
- **Destination Address of the packet,** the Layer 3 address of the computer system or device, the network packet is trying to reach
- **Type of Traffic,** the specific layer 7 network protocols being used to communicate between the source and destination systems or devices.
- **Action,** such as Deny or Permit the packet, or Drop the packet

Note: Firewall configuration must end with the rule to block all packets and connections unless the traffic type and connections have been explicitly permited

Firewall rule sets should be built to be as specific as possible with regards to the network traffic they control. Rule sets should be kept as simple as possible, so as not to accidentally introduce holes in the firewall that might allow unauthorized or unwanted traffic to traverse a firewall.

The firewall rule set should always explicitly block the following types of traffic

- Any protocol that is not need in network for ingress traffic should not be allowed.
- Any protocol that is not need in network for egress traffic should be not being allowed.
- Inbound traffic cont aining source address which is sam e as t he address of the firewall system itself.

- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. This type of packet likely represents some type of spoofing attempt.
- If possible block inbound traffic containing ICMP traffic.
- Inbound or Outbound traffic from a system using a source address that falls within the address ranges reserved for private networks. For reference purposes, RFC 1918 reserves the following address ranges for private networks

  10.0.0.0 to 10.255.255.255 (Class A)
  172.16.0.0 to 172.31.255.255 (Class B)
  192.168.0.0 to 192.168.255.255 (Class C)

- Inbound traffic containing IP Source Routing information. Source Routing is a mechanism that allows a system to specify the routes a piece of network traffic will employ while traveling from the source system to the destination system. From a security standpoint, source routing has the potential to permit an attacker to construct a network packet that bypasses firewall controls.
- Inbound or Outbound network traffic containing a source or destination address of 127.0.0.1 (Local host). Such traffic is usually some type of attack against the firewall system itself.
- Inbound or Outbound network traffic containing a source or destination address of Some operating systems interpret this address as either local host or as a broadcast address, and these packets can be used for attack purposes.
- Inbound or Outbound traffic containing directed broadcast addresses.
- Inbound traffic containing port number between 137 to 139 and 445 should strictly blocked.

1.0 Overview

Definitions

Term	Definition
Blogging:	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam:	Unauthorized and/or unsolicited electronic mass mailings.
Administration Account:	Any account that is for the administration of an operating system or application
Email:	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email:	Email resent from an internal network to an outside point.
Chain email or letter:	Email send out multiple copies to successive people.
Sensitive information:	Information is considered sensitive if it can be damaging to RESPL or its customers' reputation or market standing. Examples include, but are not limited to, personal identifiers and, financial information
Virus warning:	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure:	The intentional or unintentional revealing of restricted information to people, both inside and outside RESPL who do not have a need to know that information.

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs (including hard drive-based MP3 players); optical disks such as CD andDVD disks; floppy disks and any commercial music and software disks not provided by RESPL.

Encryption: A procedure used to convert data from its original form to a format that is unreadable and /or unusable to anyone without the tools/information needed to reverse the encryption process.

Malware: Software of malicious intent/impact such as viruses, worms, and spyware.

DMZ: De- Militarized Zone. A network segment external to the corporate production network.

Single sign-on: Single sign-on is a termed used to identify a process by which a user need only log in once for access to all information with a network. This is typically accomplished with some type of centralized authentication point to which all applications, including network operating systems, are able to verify the identity of the individual requesting access to the resources it controls.

Data Sanitization: Data sanitization is the process of deliberately, permanently, irreversibly removing or destroying the data stored on a memory device.

Accept*:* The firewall passes the packet through the firewall as requested.

Deny: The firewall drops the packet, without passing it through the firewall. Once the packet is dropped, an error message is returned to the source system.

Drop: The firewall not only drops the packet, but it does not return an error message to the source system. This particular action is used to implement the black hole methodology in which a firewall does not reveal its presence to an outsider.

Inbound traffic: Traffic that is coming from untrusted zone (Internet) to trusted zone (local network)

Outbound traffic: Traffic that is leaving from trusted zone (local network) to untrusted zone (Internet)

DATA SECURITY AND PRIVACY POLICY FOR INSTANT IT TECHNOLOGY

1. Introduction: At Radiate E Services Pvt Ltd, we recognize the importance of data security and privacy for our clients, employees, and stakeholders. This Data Security and Privacy Policy outlines our commitment to safeguarding sensitive information, ensuring compliance with relevant data protection laws, and maintaining the trust of those who entrust us with their data.

2. Scope: This policy applies to all aspects of data processing carried out by Radiate Organization, including client information, employee data, and any other data collected during our operations.

3. Data Collection and Usage: 3.1 Purpose Limitation: We collect and process data solely for specified and legitimate purposes. Data is not used for any other purpose without obtaining appropriate consent.

3.2 Consent: We ensure that individuals' explicit and informed consent is obtained before collecting and processing their personal data, wherever required.

3.3 Data Minimization: We collect only the minimum amount of data necessary for the intended purpose and avoid excessive data collection.

3.4 Client Data: Client data is used only to provide the services requested by the client and is not shared with third parties without prior consent.

4. Data Security: 4.1 Physical Security: We maintain secure facilities and access controls to prevent unauthorized physical access to data storage areas.

DATA SECURITY AND PRIVACY POLICY FOR INSTANT IT TECHNOLOGY

4.2 Information Security: Data is protected using industry-standard encryption techniques during storage and transmission.

4.3 Access Control: Access to sensitive data is restricted to authorized personnel only. Access privileges are granted on a need-to-know basis.

4.4 Employee Training: Our employees undergo regular data security and privacy training to ensure they understand and follow security protocols.

5. Data Retention: 5.1 Retention Period: Data is retained only for as long as necessary to fulfill the purpose for which it was collected, unless a longer retention period is required by law.

5.2 Data Disposal: Data is securely disposed of when it is no longer needed, following approved data disposal procedures.

6. Data Sharing: 6.1 Third Parties: Data is shared with third parties only when necessary for providing services and is done with proper contractual safeguards in place.

6.2 Client Agreements: Agreements with clients include provisions outlining data processing responsibilities and data protection commitments.

7. Compliance: 7.1 Legal Requirements: We adhere to all relevant data protection laws and regulations in the jurisdictions where we operate.

DATA SECURITY AND PRIVACY POLICY FOR INSTANT IT TECHNOLOGY

7.2 Monitoring and Audit: We conduct regular audits and assessments of our data security and privacy practices to ensure compliance.

8. Individual Rights: 8.1 Access and Correction: Individuals have the right to access their personal data and request corrections if necessary.

8.2 Erasure: Individuals have the right to request the deletion of their personal data in accordance with applicable laws.

9. Data Breach Response:

9.1 Notification: In the event of a data breach, affected parties and relevant authorities will be notified promptly, and appropriate measures will be taken to mitigate the impact.

10. Continuous Improvement: We are committed to continuously improving our data security and privacy practices based on evolving technologies, threats, and regulations.

11. Contact Information: For any inquiries or concerns regarding data security and privacy, please contact our Data Protection Officer at info@instantittechnology.com

12. Policy Review: This policy will be reviewed regularly to ensure its relevance and effectiveness in maintaining data security and privacy. This Data Security and Privacy Policy is effective as of 1 Aug 2023

Acceptable Usage Do's & Don'ts:-

Do's	Don'ts
Use accesses for valid business purposes only	Use company resources for personal purposes
Keep activity to least privilege and need to know basis	Send company data/IP to personal email ID's unless authorized
Visit authorized websites for business purposes only	Copy company data/IP to personal drives, systems etc.
Take approvals in case access to restricted sites are required for business purposes	Use company resources to access, download, or distribute pornographic, obscene, defamatory, discriminatory, harassing, or other inappropriate materials of any kind
Follow clear desk and clear screen practices	Use company resources to download, store or transmit materials that infringe any copyright, trademark, licensing agreement, or other proprietary right
Follow security protocols	Circumvent security controls

Note: The above list is for understanding purposes and is not comprehensive to cover all Do's and Don'ts as per company policies, procedures, or standards.

Acknowledgement:-

I hereby acknowledge that I have read Company's IT Acceptable Use Policy and I agree to adhere to all the terms in this policy. I will take all precautions to ensure confidentiality, non-disclosure, and protection of all non-public information of Company always. Any violation may lead to disciplinary or legal actions not limited to termination.

Employee Name :-____

Employee ID :-____

Manager Name :- ____

Department :- ____

Signature :- ____

Date :-____