Document Information

Title: Information & Security Policy	Version No: 1
Prepared For : Nell Infotech Pvt Ltd	Version Date: 23/8/2023
Author: Manisha Jadhav	Date Created: 18/08/2023
Reviewed By: Sheetal Jadhav	Review Date: 21/08/23

Version History

Version Number	Version Date	Revised By	Description
1	23/08/2023		Initial Document created

Author	**Reviewed by**	**Approved by**
Manisha Jadhav	Sheetal Jadhav	Sheetal Jadhav
Nell Infotech	Nell Infotech	Nell Infotech
Director[HR & Operation]	CEO	CEO

1. Contents

Introduction

INFORMATION AND SECURITY POLICY

Introduction

Information security is a holistic discipline, meaning that its application (or lack thereof) affects all facets of an organisation or enterprise. The goal of the **Nell Infotech Pvt. Ltd.** Information Security Program is to protect the ***confidentiality***, ***integrity***, **and** ***availability*** of the data used within the organisation while enhancing the way we conduct business. Protection of confidentiality, integrity, and availability is a basic principle of information security, and can be defined as:

- **Confidentiality** – Ensuring that information is accessible only to those entities that are authorised to have access, many times enforced by the classic "need to know" principle.
- **Integrity** – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- **Availability** – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorised entity.
-

Nell Infotech Pvt. Ltd. has recognised that our business information is a critical asset. As such, our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control, and protect its business information assets and those information assets entrusted to **Nell Infotech Pvt Ltd.** by its stakeholders, partners, customers, and other third parties.

The **Nell Infotech Pvt Ltd.** Information Security Program is built around the information contained within this policy and its supporting policies.

Purpose

The purpose of the **Nell Infotech Pvt Ltd.** Information Security Policy is to describe the actions and behaviours required to ensure that due care is taken to avoid inappropriate risks to **Nell Infotech Pvt Ltd.**, its business partners, and its stakeholders.

Audience

The **Nell Infotech Pvt. Ltd.** Information Security Policy applies equally to any individual, entity, or process that interacts with any **Nell Infotech Pvt. Ltd.** Information Resource.

Table of Contents

6. Password management policy:-

Outlines the requirements for an organisation's proper and secure handling of user credentials. Applies to all of the organisation's users and third parties possessing credentials to the organisation's accounts.

7. Incident response policy:-

Guides the organisation's response to a data security incident. Applies to an organisation's security officers and other employees, information systems, and data.

8 Hardware & Electronic Media Disposal Policy:-

Guides the organisation to proper and secure disposal of Hardware & Electronic Media.

1. Acceptable Use Of Information System Policy

Overview

Data, electronic file content, information systems, and computer systems at **Nell Infotech Pvt. Ltd.** must be managed as valuable organisational resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to **Nell Infotech Pvt. Ltd.**'s established culture of openness, trust, and integrity. IT is committed to protecting **Nell Infotech Pvt Ltd.**'s authorised users, partners, 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 File Transfer Protocol (FTP), are the property of **Nell Infotech Pvt Ltd.**

These systems are to be used for business purposes in serving the interests of **Nell Infotech Pvt Ltd.** and of its clients and members during normal operations.

Effective security is a team effort involving the participation and support of every **Nell Infotech Pvt. Ltd.** employee, volunteer, 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 activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at **Nell Infotech Pvt Ltd.** These rules are in place to protect the authorised user and **Nell Infotech Pvt Ltd.** Inappropriate use exposes **Nell Infotech Pvt Ltd.** to risks, including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct **Nell Infotech Pvt Ltd** business or interact with internal networks and business systems, whether owned or leased by **Nell Infotech Pvt Ltd.**, the employee, or a third party.

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at **Nell Infotech Pvt Ltd.**, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with **Nell Infotech Pvt Ltd.** policies and standards, local laws, and regulations.

Policy Detail

Ownership of Electronic Files

All electronic files created, sent, received, or stored on **Nell Infotech Pvt Ltd.** owned, leased, or administered equipment or otherwise under the custody and control of **Nell Infotech Pvt Ltd.** are the property of **Nell Infotech Pvt Ltd.**

Privacy

Electronic files created, sent, received, or stored on **Nell Infotech Pvt. Ltd.** owned, leased, or administered equipment, or otherwise under the custody and control of **Nell Infotech Pvt Ltd.** are not private and may be accessed by **Nell Infotech Pvt. Ltd.** IT employees at any time without knowledge of the user, sender, recipient, or owner.

Electronic file content may also be accessed by appropriate personnel in accordance with directives from Human Resources or the President/CEO.

General Use and Ownership

Access requests must be authorised and submitted by departmental supervisors for employees to gain access to computer systems. Authorised users are accountable for all activity that takes place under their username.

Authorised users should be aware that the data and files they create on the corporate systems immediately become the property of **Nell Infotech Pvt Ltd.**. Because of the need to protect **Nell Infotech Pvt. Ltd.**'s network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to **Nell Infotech Pvt Ltd.**

For security and network maintenance purposes, authorised individuals within the **Nell Infotech Pvt Ltd.** IT Department may monitor equipment, systems, and network traffic at any time.

Nell Infotech Pvt Ltd.'s IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Nell Infotech Pvt Ltd.'s IT Department reserves the right to remove any non-business-related software or files from any system.

Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with this policy and the following policies:

- Account Management
- Anti-Virus
- Owned Mobile Device Acceptable Use and Security
- E-mail
- Internet
- Safeguarding Member Information
- Personal Device Acceptable Use and Security
- Password
- Cloud Computing
- Wireless (Wi-Fi) Connectivity
- Telecommuting

System-level and user-level passwords must comply with the Password Policy. Authorised users must not share their **Nell Infotech Pvt Ltd.** login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes.

Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorised users may access, use, or share **Nell Infotech Pvt Ltd** proprietary information only to the extent it is authorised and necessary to fulfil the users' assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.

All users must lock down their PCs, laptops, and workstations by locking (control-alt- delete) when the host will be unattended for any amount of time. Employees must log off or restart (but not shut down) their PC after their shift.

Nell Infotech Pvt Ltd's proprietary information stored on electronic and computing devices, whether owned or leased by **Nell Infotech Pvt Ltd.**, the employee, or a third party, remains the sole property of **Nell Infotech Pvt Ltd.** All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorised disclosure of **Nell Infotech Pvt Ltd's** proprietary information to their immediate supervisor and/or the IT Department.

All users must report any weaknesses in **Nell Infotech Pvt Ltd's** computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the IT Department.

Authorised users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which **Nell Infotech Pvt. Ltd.** may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, volunteer/director, contractor, consultant, or temporary employee of **Nell Infotech Pvt Ltd** authorised to engage in any activity that is illegal under local, state, federal, or international law while utilising **Nell Infotech Pvt. Ltd.** owned resources.

System and Network Activities

The following activities are prohibited by users, with no exceptions:

- 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 **Nell Infotech Pvt. Ltd.**
- Unauthorised copying of copyrighted material, including, but not limited to, digitisation and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which **Nell Infotech Pvt. Ltd.** or the end user does not

have an active license, is prohibited. Users must report unlicensed copies of installed software to IT.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- 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.
- Using a **Nell Infotech Pvt. Ltd.** computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Attempting to access any data, electronic content, or programs contained on **Nell Infotech Pvt. Ltd.** systems for which they do not have authorisation, explicit consent, or implicit need for their job duties.
- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of **Nell Infotech Pvt. Ltd.** IT.
- Installing or using non-standard shareware or freeware software without **Nell Infotech Pvt. Ltd.** IT approval.
- Installing, disconnecting, or moving any **Nell Infotech Pvt. Ltd.** owned computer equipment and peripheral devices without prior consent of **Nell Infotech Pvt. Ltd.**'s IT Department.
- Purchasing software or hardware for **Nell Infotech Pvt. Ltd** use without prior IT compatibility review.
- Purposely engaging in an activity that may;
    - degrade the performance of information systems;
    - deprive an authorised **Nell Infotech Pvt. Ltd.** user access to a **Nell Infotech Pvt. Ltd.** resource;
    - obtain extra resources beyond those allocated; or
    - circumvent **Nell Infotech Pvt. Ltd.** computer security measures.
- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, **Nell Infotech Pvt. Ltd.** users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on **Nell Infotech Pvt. Ltd.** information systems. The **Nell Infotech Pvt. Ltd.** IT Department is the only department authorised to perform these actions.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- 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.

Access to the Internet at home, from a **Nell Infotech Pvt. Ltd.** owned computer, must adhere to all the same policies that apply to use from within **Nell Infotech Pvt Ltd** facilities. Authorised users must not allow family members or other non-authorised users to access **Nell Infotech Pvt Ltd** computer systems.

Nell Infotech Pvt Ltd information systems must not be used for personal benefit.

2. Data Management Policy

Purpose

Managing data within an enterprise includes data classification, inventory, handling, retention, and disposal. The *Data Management Policy* provides the processes and procedures for governing data within the enterprise. This includes creating a data inventory and classifying data based on sensitivity. Additionally, procedures for securely protecting data from unauthorised access or modification, alongside appropriate methods for how users should handle their data during their day-to-day work activities. Finally, authorised methods to destroy and remove data from the enterprise are discussed.

Responsibility

- The IT business unit is responsible for managing the enterprise's data, as this information is housed on workstations and servers primarily maintained by IT. Information owners are responsible for coordinating data maintenance activities with IT.
- Users have the responsibility to protect data associated with their role from unauthorised access and disclosure. IT is responsible for informing all users of their responsibilities associated with protecting data entrusted to them.

Policy

Data Inventory

1. IT must conduct an inventory of data on an annual basis.
    a. All sensitive data must be marked accordingly in the data inventory.
    b. A data owner must be associated with all data tracked within the inventory.
    c. Data with specific data retention needs must be labelled accordingly.
2. All data owners are required to contact IT upon the creation of, or obtaining, sensitive data to ensure the data is tracked within the data inventory.

Data Classification

1. IT must establish and enforce labels for sensitive data.
2. IT must review data classification labels and their usage on an annual basis.

Data Protection

1. IT must configure access control lists on enterprise assets in accordance with the user's need to know. This is to include laptops, smartphones, tablets, centralised file systems, remote file systems, databases, and all applications.
2. Sensitive data must be encrypted on all user devices.

Data Handling

1. IT must develop and maintain a written data retention plan.
    a. All data and documents must be preserved for the appropriate amount of time as dictated by regulatory, legal, and business requirements.

Data Disposal

1. IT, or other authorised parties, must destroy data that has outlasted their specified retention timeframes.
2. All users are required to contact IT before disposing of sensitive data.
3. Non-sensitive data may be disposed of without speaking to IT via common destruction methods (e.g., trash, commonplace deletion from a computer system).
4. Sensitive data destruction must be performed in a manner that preserves confidentiality.
    a. Reports, correspondence, and other printed media:
        i. Shredding – Documents must be shredded using IT-approved cross-cut shredders,
        ii. Shredding Bins – Disposal must be performed using locked bins located on-site using an IT-approved shredding service, or
        iii. Incineration – Materials are physically destroyed using an IT-approved incineration service.
    b. Portable Media (e.g., Solid State Drives (SSDs), digital video discs (DVDs), universal serial bus (USB) data storage devices):
        i. Physical Destruction – Complete destruction of media by means of shredding, crushing, or disassembling the asset and ensuring no data can be recovered.
    c. Hard Disc Drives (HDDs) and other magnetic media to include printer and copier hard drives:
        i. Overwriting – Using a program to write binary data sector by sector onto the media, or
        ii. Physical Destruction – Crushing, disassembling, or degaussing the asset to ensure no data can be extracted or recreated.
    d. Tape Cartridges
        i. Degaussing – Using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state, or
        ii. Physical Destruction – Complete destruction of the tapes.
    e. Third-party service provider systems (e.g., cloud services) must be disposed of by first requesting the appropriate methods to permanently delete data stored in their systems, and then performing those actions according to the received instructions.

5. All destruction of data must be logged in the data inventory, when applicable.

a. IT must obtain proof of destruction if using a third-party disposal contractor.

3.Network Security Policy

Overview

This policy is to protect **Nell Infotech Pvt Ltd**'s electronic information from being inadvertently compromised by authorised personnel connecting to the **Nell Infotech Pvt. Ltd.** network locally and remotely via VPN**.**

Purpose

The purpose of this policy is to define standards for connecting to **Nell Infotech Pvt. Ltd.**'s network from any host. These standards are designed to minimise the potential exposure to **Nell Infotech Pvt Ltd** from damages, which may result from unauthorised use of **Nell Infotech Pvt Ltd's** resources.

Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical **Nell Infotech Pvt. Ltd.** internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, and cable modems, etc.

Audience

This policy applies to all **Nell Infotech Pvt Ltd.** employees, volunteers/directors, contractors, vendors, and agents with a computer or workstation used to connect to the **Nell Infotech Pvt Ltd** network. This policy applies to remote access connections used to do work on behalf of **Nell Infotech Pvt Ltd,** including reading or sending email and viewing intranet resources.

Policy Detail

Users are permitted to use only those network addresses assigned to them by **Nell Infotech Pvt. Ltd.**'s IT Department.

Remote users may connect to **Nell Infotech Pvt Ltd** Information Systems using only protocols approved by IT. Users inside the **Nell Infotech Pvt Ltd** firewall may not be connected to the **Nell Infotech Pvt Ltd.** network at the same time a remote connection is used to an external network.

Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point on the **Nell Infotech Pvt Ltd** network without **Nell Infotech Pvt Ltd.** IT approval.

Users must not install network hardware or software that provides network services without **Nell Infotech Pvt Ltd.** IT approval. Non-**Nell Infotech Pvt Ltd** computer systems that require network connectivity must be approved by **Nell Infotech Pvt Ltd.** IT.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, **Nell Infotech Pvt Ltd.** users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the **Nell Infotech Pvt Ltd.** network infrastructure. Only the IT Department is permitted to perform these actions.

Users are not permitted to alter network hardware in any way.

4.Access Control Policy

Overview

Physical access controls define who is allowed physical access to **Nell Infotech Pvt Ltd.** facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exits that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

Purpose

This policy applies to all facilities of **Nell Infotech Pvt Ltd.** within which information systems or information system components are housed. Specifically, it includes:

- Data centres or other facilities for which the primary purpose is the housing of IT infrastructure
- Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure
- Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure

Policy Detail

Access to facilities, information systems, and information system display mechanisms will be limited to authorised personnel only. Authorisation will be demonstrated with authorisation credentials (badges, identity cards, etc.) that have been issued by **Nell Infotech Pvt. Ltd.**

Access to facilities will be controlled at defined access points with the use of card readers and locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorised personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility without prior authorisation, and all deliveries and removals will be logged.

A list of authorised personnel will be established and maintained so that newly authorised personnel are immediately appended to the list, and those personnel who have lost authorisation are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.

If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorisation, must be positively identified, and must have their authorisation verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities must be monitored at all times.

5.Remote Access Policy

Policy Details:

It is the responsibility of **Nell Infotech Pvt Ltd.** employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to Nell Infotech Pvt. Ltd.'s corporate network, to ensure that their remote access connection is given the same consideration as the users' on-site connection to **Nell Infotech Pvt. Ltd**.

General access to the Internet through the **Nell Infotech Pvt Ltd** network is permitted for employees who have flat-rate services and only for business purposes. **Nell Infotech Pvt Ltd.** employees are responsible for ensuring that they:

- Do not violate any **Nell Infotech Pvt. Ltd.** policies
- Do not perform illegal activities
- Do not use the access for outside business interests

Nell Infotech Pvt Ltd. employees bear responsibility for the consequences should access be misused.

6.Password Policy

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 **Nell Infotech Pvt Ltd.**'s entire corporate network. As such, all **Nell Infotech Pvt Ltd.** employees or volunteers/directors (including contractors and vendors with access to **Nell Infotech Pvt Ltd.** systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

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

Audience

This policy applies to all personnel or volunteers/directors 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 **Nell Infotech Pvt Ltd** facility, have access to the **Nell Infotech Pvt Ltd.** network, or store any non-public **Nell Infotech Pvt Ltd.** information.

Policy Detail

User Network Passwords

- Passwords for **Nell Infotech Pvt. Ltd.** network access must be implemented according to the following guidelines:
- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~';',<>|\).
- Passwords must not be easily tied back to the account owner, such as:
- username, social security number, nickname, relative's names, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for 1 year

System-Level Passwords

- All system-level passwords must adhere to the following guidelines:
- Passwords must be changed at least every 6 months
- All administrator accounts must have 12-character passwords that must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented, listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use

Password Protection /R

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential **Nell Infotech Pvt. Ltd.** information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- **Nell Infotech Pvt Ltd.** passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.
- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT /R
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with {COMPANY-NAME}.

Application Development Standards

Application developers must ensure their programs follow security precautions in this policy and industry standards.

7.Security Incident Management Policy

Overview

Security Incident Management at **Nell Infotech Pvt. Ltd.** is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify **Nell Infotech Pvt Ltd** members of the breach.

Purpose

This policy defines the requirement for reporting and responding to incidents related to **Nell Infotech Pvt Ltd.** information systems and operations. Incident response provides **Nell Infotech Pvt Ltd.** with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

This policy applies to all information systems and information system components of **Nell Infotech Pvt. Ltd.** Specifically, it includes:

- Mainframes, servers, and other devices that provide centralised computing capabilities.
- Devices that provide centralised storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

Policy Detail

Program Organization

- **Computer Emergency Response Plans** - **Nell Infotech Pvt Ltd** management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.
- **Incident Response Plan Contents** - The **Nell Infotech Pvt Ltd** incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:
    - Specific incident response procedures
    - Business recovery and continuity procedures
    - Data backup processes
    - Analysis of legal requirements for reporting compromises
    - Identification and coverage for all critical system components
    - Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers

- **Incident Response Testing** - at least once every year, the IT Department must utilise simulated incidents to mobilise and test the adequacy of response. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.
- **Incident Response and Recovery** - A security incident response capability will be developed and implemented for all information systems that house or access **Nell Infotech Pvt. Ltd.** controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
    - Preparation
    - Detection
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
  - To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.
  - Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of the plan revision, updated plans will be distributed to key stakeholders.

- **Intrusion Response Procedures** - The IT Department must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.
- **Malicious Code Remediation** - Steps followed will vary based on the scope and severity of a malicious code incident, as determined by Information Security Management. They may include, but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.
- **Data Breach Management** - **Nell Infotech Pvt Ltd** management should prepare, test, and annually update the Incident Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.
- **Incident Response Plan Evolution** - The Incident Response Plan must be updated to reflect the lessons learned from actual incidents. The Incident Response Plan must be updated to reflect developments in the industry.

8. Hardware & Electronic Media Disposal Policy

Overview

Nell Infotech Pvt. Ltd to ensure the proper disposition of all non-leased **Nell Infotech Pvt. Ltd.** IT hardware and media capable of storing member information. Improper disposition can lead to potentially devastating fines and lawsuits, as well as possible irreparable brand damage.

Purpose

Nell Infotech Pvt. Ltd. owns surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, which are covered by this policy.

Where assets have not reached the end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

Nell Infotech Pvt Ltd's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and **Nell Infotech Pvt Ltd**'s upgrade guidelines.

All disposition procedures for retired IT assets must adhere to company-approved methods.

Policy Detail

Co-ordinated by **Nell Infotech Pvt Ltd'**s IT Department. The IT Department is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitisation, reselling, recycling, or destruction of the equipment. IT is also responsible for the chain of custody in acquiring credible documentation from contracted third parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations.

It is the responsibility of any employee of **Nell Infotech Pvt Ltd.**'s IT Department, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the Hardware and Electronic Media Disposal Procedure.. All dispositions must be done appropriately, responsibly, and according to IT lifecycle standards, as well as with **Nell Infotech Pvt Ltd.**'s resource planning in mind. Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)
- Printers

- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives / Flash memory
- Other portable storage device.