Data Protection & Cyber Security Protocols

Manoj Vaibhav Gems 'N' Jewellers Limited (VAIBHAV)

Author Name	Designation	Version	Date
Y Sandeep Krishna	AGM-IT	2.3	07-07-2022

Contents

1. Introduction.

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Manoj Vaibhav Gems 'N' Jewellers Limited ("Vaibhav") has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

2. Purpose.

The purpose of this policy is to

- protect Vaibhav data and infrastructure,
- outline the protocols and guidelines that govern cyber security measures,
- define the rules for company and personal use, and
- list the company's disciplinary process for policy violations.

3. Scope.

This policy applies to all of Vaibhav's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

4. Confidential Data.

Vaibhav defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

5. Information Security Policy

At Vaibhav Jewellers, we handle customer information and ensure that we collect, keep, and manage data concerning individual rights and customer privacy reasonably and transparently. Our staff is committed to safeguarding client data and ensuring a secure environment for processing customer information.

We reserve the right to monitor, access, examine, audit, copy, store, and delete all electronic communications, systems, and network traffic.

We pledge to monitor the usage of Company resources like e-mail and the internet to prevent inappropriate or unlawful conduct.
Employees handling Sensitive customer data ensure:

- Not to divulge personnel records without authorisation;
- Protect confidential consumer information;
- We always maintain secure passwords and accounts;
- We do not install unapproved software or hardware, including modems and wireless connections, without notifying IT Team beforehand.
- Our employees never leave their desk without cleaning crucial customer data and always lock the computer screen when they're away;
- Incidents with information security are always reported immediately to the IT Team.

6. Acceptable Use Policy

Publication of an Acceptable Use Policy is not intended to impose limits but to preserve the existing culture of openness, trust, and integrity. We are obligated to safeguard employees, vendors, and the company against illegal acts performed by other parties, whether intentionally or unintentionally. Our IT department maintains a list of acceptable technologies, devices, and employees with access to company-issued equipment.

The Employees are responsible for the following:

Each team member is responsible for making prudent decisions while using business time. They are only authorised to utilise technology by obtaining the necessary credentials. Staff members take all the required measures to ensure that sensitive information, such as customer, financial, and stakeholder data, is protected from unauthorised access.

To top it all off, they never share passwords or accounts with anyone. Each employee's responsibility is to safeguard their unique set of login information. We take extra measures to protect data stored on portable laptops. Our staff members are trained to exercise extreme caution when opening attachments in unsolicited e-mails. These messages may contain malicious files such as viruses, e-mail bombs, or Trojan horse malware.

7. Protect Stored Data

Important customer/stakeholder data kept and handled by staff is secured against unauthorised access. Under the direction of the IT team, any sensitive customer data that our brand no longer requires for business purposes is discarded in a secure and irrecoverable manner.

8. Access to the vital customer data

Access to critical customer data is strictly controlled and authorised.

- Our team limits the display of customer Account Numbers (Credit/Debit/Bank Account Numbers) to the last 4 digits.

- Employees who are authorised to perform essential job responsibilities are granted access to customer data.

9. Physical Security

To prevent unauthorised individuals from getting sensitive data, we restrict access to sensitive information on both hard and soft media forms. All equipment are adequately safeguarded and secured so it cannot be tampered with.

Employees ensure the following:

Every employee possesses the necessary authorisations and permissions to operate the technology we deploy. Security measures are in place to ensure that confidential information, such as that belonging to customers and other stakeholders, is kept safe from prying eyes. Staff members check to ensure technologies are used in appropriate network zones.

Everyone on the team respects the privacy of users' login information and never shares their credentials. Workers are responsible for keeping their login information private. Only authorised employees at Vaibhav Jewellers have access to and are responsible for disseminating media containing confidential customer information. Those who work with POS terminals are obligated to report any suspicious activity or evidence of tampering to the IT Department.

10. Security Awareness and Procedures

Maintaining a high degree of security awareness requires adherence to the policies and procedures listed below.

We restrict the disclosure of sensitive information such as:

a. Customer data
b. Company financial data
c. Company sales data etc.
d. Personal information
e. Hierarchy of company staff
f. Supplier Information
g. Any other Important Information which is identified from time to time

11. System and Password Policy

User having access to Workstations and Servers is responsible for taking the tasks specified below.

- A server configuration standard is designed following industry-acceptable hardening requirements Configurations of servers are modified.
- Server configurations consist of typical security parameter settings.
- The server configuration standard is applied to newly configured systems.
- When deploying the system/device into the VAIBHAV network, all vendor-default accounts and passwords for the machine are updated. All nonessential services and user/system accounts are disabled. Before deploying a server on a network, all unnecessary default accounts are removed or disabled.
- We configure security parameter settings on System components suitably.
- We eliminate all redundant functions (scripts, drivers, features, subsystems, file systems, web servers etc.).
- All extra services, protocols, daemons, etc. will be disabled if the server is not using them.
- Users enter passwords to access the company network or any other electronic equipment.
- All user IDs for resigned or terminated personnel are instantly deleted or removed.
- Our team modifies all server- and user-level passwords every three months.
- We assign new users a unique password, and they are prompted to change it upon their first login.
- No system components are administered using group-shared or generic user accounts, passwords, or other authentication techniques.
- Where SNMP is employed, the community strings are defined as anything other than the Standard defaults of "public," "private," and "system." Additionally, the passwords used to log in interactively must be distinct from the community strings.
- All non-console administrative access use appropriate technologies such as SSH, VPN, etc., or strong encryption will be activated before requesting the administrator password.
- System services and parameters are configured to prevent the usage of vulnerable technology.
- Users are instructed to select passwords that are difficult to guess. A strong password is usually a longer one (never less than 8 characters for standard users and 12 for power users)—personnel involved in transactions and approvals with other financial institutions.
- To prevent network analysis assaults, the servers are cryptographically secured. Secure protocols include the encrypted Netware login.

12. Anti-virus policy

- All machines are configured with the most current anti-virus software. Users complain to the IT Team if their Anti-Virus software is out-of-date. Immediately
- Before using any removable media (such as USB flash drives and others), it is scanned for viruses.
- We avoid opening e-mail attachments from unknown or dubious senders. We ensure that all such e-mails and attachments are deleted from the inbox and trash bin. No one is permitted to forward any suspected virus-infected e-mail.

13. Remote Access policy

The IT Team is responsible for granting remote access rights to our business network and ensuring that the user's remote access connection is identical to their on-site connection. Employees are prohibited from sharing their access credentials unless authorised

14. Incident Response Plan

The term 'Security Incident' refers to any incident (accidental, willful, or purposeful) involving your communications or information processing systems. The attacker could be a hostile stranger, a competitor, or a disgruntled employee whose purpose is to steal information.

Employees notify the IT department and their immediate supervisors of any potential security breaches. Our IT team also tracks any unauthorised or remote access to our systems or servers regularly and monitor the same

15. User Access Management

- Access is granted to a new user via a formal user registration procedure that begins with a formal notification from HR.
- Each user is assigned a unique user ID, allowing individuals to be linked and held accountable for their actions. Group IDs are only permitted when appropriate for the tasks being performed.
- All employees have a standard degree of access; further services may be accessible with special authorisation from IT/Management. The user's job function determines the level of access to customer/financial data.
- Service requests for new employees are submitted in writing (e-mail or physical copy) with the consent of an immediate manager.
- The IT Team provides access to all VAIBHAV systems, which is only be activated after completing all necessary procedures.
- When an employee quits the company, their system login credentials are immediately revoked.

- HR notifies the IT Team of the employee Exit and leaving date as part of the employee Exit procedure.

16. Access Control Policy

- Our Access Control systems are in place to protect the interests of all users of VAIBHAV computer systems by providing a safe, secure and readily accessible environment in which to work.

- We do not permit generic or group IDs but grant them under exceptional circumstances. If sufficient, we put other controls on access in place.

- We accord access rights following the principles of least privilege and need-to-know basis.

- Users placing information on digital media or storage devices or maintaining a separate database only do so where such action follows the data's classification.

- Users are obligated to report instances of non-compliance to the IT team

- We have access to The Company IT resources and services by providing a unique Active Directory account and complex password.

- We manage password issuing, strength requirements, changing and control through formal processes. We handle password length, complexity and expiration times through Windows Active Directory Group Policy Objects.

- We have limited access to Confidential, Restricted and Protected information to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.

- Our users are familiar with and abide by security policies, standards and guidelines for appropriate and acceptable usage of systems.

- Access for remote users is subject to authorisation by IT Team and is provided following the Remote Access Policy. No uncontrolled external access is permitted to any network device or networked system.

- We control access to data according to the data classification levels

17. Security Guidelines

a) For Business

- We have installed a dedicated, actively managed firewall. A firewall limits the potential for unauthorised access to a network and computers.

- We have installed well-known and supported anti-virus and desktop firewall software on all computer systems. Look for names you know and read independent reviews of all products you use.

- We ensure that computers are regularly patched, mainly operating systems and critical applications, with security patches. It is highly recommended to sign up for automatic operating system updates for the operating system and many non-operating system applications.

- We change the default login names and PINs on routers, firewalls, and other network equipment and software on a regular basis

- We monitor log files, especially proxy server logs, for unauthorised/suspicious Internet connections coming to and leaving the network.

- We implemented safe listing methods to prevent the system for online companying from going to any site/address that does not have a documented business need.

- We avoid using a wireless network for financial transactions. We are using a wireless network to enforce security measures such as enabling encryption and MAC address filtering, changing the service set identifier (SSID) and turning off SSID broadcasting.

- We turn off and remove services that are not needed on computers. We allow the use of CDs, DVDs, and USB devices for legitimate business needs if there is no alternative, and we will strictly monitor it.

- We block Internet plug-ins on the computers that access online companying accounts. Disabling Flash, scripts, pop-up windows, etc.,

- We ensure that employees cannot override or circumvent security software.

- We only approve company applications that will be deployed on computers and patched regularly.

- If we have employees who use laptops, we implement software that determines if devices have been infected before allowing them back into our network (Network Admission Control – NAC).

b) For Employees - General

- We use an updated Internet browser with 128-bit encryption that supports secure and private transactions.

- We use a software or hardware firewall to protect our computers from network intrusion.

- We maintain and run anti-spyware / anti-malware / anti-virus software to detect new threats.

- If a computer is on a wireless network (home or public), we ensure that the router settings are secure (encrypted). Individuals can intercept unencrypted signals using scanning devices and view or obtain personal information.

- We use caution when downloading files, installing software, or opening e-mail attachments from unverified or unknown sources. Many files contain spyware or key-logging programs that send information back to a malicious site.

- We are suspicious of e-mails purporting to be from a Financial Institution, government department or other agency requesting account information, account verification or companying access credentials such as User IDs, PINs, Codes and similar information. We know that opening file attachments or clicking on web links in suspicious e-mails could expose the system to malicious code that could hijack the network.

- We clear the browser cache before starting an online session to eliminate copies of web pages stored on the hard drive.

- We always lock our computers when we leave them unattended. We have set the computer to lock automatically after a period of inactivity, e.g. 5 minutes.

- We properly dispose of old computers and ensure all sensitive information is removed from the hard drive.

c) For Employees – E mail

- Suppose a team member believes they may have submitted personal or account information in response to a fake e-mail or website. In that case, they are instructed to report the incident immediately, change their PINs, and routinely monitor their account activity.

- The savvy team at Vaibhav Jewellers knows the need to avoid clicking on links shared via e-mails. They always manually enter the address into the browser instead.

- Most computer files include filename extensions, such as ".doc" or ".jpg" for papers and images. Our staff has been warned not to open any file that looks to have two extensions, such as "hello.doc.pdf." etc. It is quite likely to be a malicious file.

- We prohibit the opening of e-mail attachments with the ".exe", ".pif", and ".vbs" extensions, etc. These are the file extensions for executable programmes, typically malicious.

- Before giving their e-mail address to a dubious website, our staff exercise caution and discretion, sharing their e-mail address increases their likelihood of receiving phishing e-mails.

- We evaluate the legitimacy of all demands for sensitive personal, financial, or account information, especially if they are urgent or threatening in nature.

18. Disciplinary Action

Employees who violate the standards, policies, and procedures outlined in this document are subject to disciplinary action, ranging from warnings and reprimands to dismissal. Lack of knowledge, good intentions, or bad judgement will not be accepted as justifications for non-compliance.

* * * * * * * * * * * * *