



D.P. Jewellers

— A BOND OF TRUST SINCE 1940 —

A VENTURE OF D.P. ABHUSHAN LIMITED

CYBER SECURITY POLICY

Approving Authority Board of Directors of the Company
Review Cycle As may be decided by the Board

Cyber Security Policy

1. INTRODUCTION AND PURPOSE

The digital assets of D. P. Abhushan Limited, including information, systems, and networks, are critical to our operations, reputation, and client trust. This Cybersecurity Policy outlines the principles and rules governing the security of these assets. Its purpose is to protect D. P. Abhushan Limited from cybersecurity threats, ensure the confidentiality, integrity, and availability of information, and maintain compliance with relevant laws and regulations.

2. SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and any third parties who have access to D. P. Abhushan Limited's information systems, networks, data, or physical IT assets, regardless of their location or the device used. It covers all company-owned, leased, or managed information systems and data, whether stored on-premises or in cloud services.

3. Core Principles

- **Confidentiality:** Protect sensitive information from unauthorized access and disclosure.
- **Integrity:** Ensure the accuracy, completeness, and reliability of information and systems.
- **Availability:** Guarantee that authorized users can access information and systems when needed.
- **Compliance:** Adhere to all applicable laws, regulations, and industry standards related to data protection and cybersecurity.
- **Proactive Defence:** Implement preventative measures to minimize vulnerabilities and protect against evolving threats.
- **Risk Management:** Identify, assess, and mitigate cybersecurity risks systematically.

4. POLICY ELEMENTS

4.1 Confidential Data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

4.2 Protect Personal and Company Devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.

- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

4.3 Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- E-mail and internet usage must be professional and for business purposes.
- Downloading unauthorized software or accessing illegal/offensive content is prohibited.
- Users must be vigilant against phishing, spam, and suspicious emails. Do not click on suspicious links or open attachments from unknown senders.
- Check email and names of people they received a message from to ensure they are legitimate.
- If an employee isn't sure that the e-mail they have received is safe or not, they can refer to our IT Specialist.

4.4 Malware Protection

- All company endpoints and servers must have approved anti-malware software installed and kept up-to-date.
- Scheduled scans must be performed regularly.
- Users must exercise caution when opening email attachments or clicking on links from unknown sources. Any suspected malware incidents must be reported immediately.

4.5 Data Backup and Recovery

- Critical data will be regularly backed up to secure, offsite locations to ensure recoverability in case of data loss or system failure.
- Backup integrity and recovery procedures will be tested periodically.

4.6 Incident Response

- All cybersecurity incidents (e.g., data breaches, malware infections, unauthorized access attempts) must be reported immediately to the IT Department.
- A formal Incident Response Plan will be maintained and periodically tested to ensure prompt and effective handling of security incidents.

4.7 Vendor and Third-Party Security

- Third-party vendors and service providers with access to D. P. Abhushan Limited's systems or data must comply with this policy and demonstrate adequate security controls.
- Security requirements will be included in all relevant contracts.

4.8 Mobile Device Security

- All mobile devices used for company business, whether company-owned or personal (BYOD), must comply with the company's mobile device security guidelines (e.g., strong passwords, encryption, remote wipe capabilities).
- Confidential company data must not be stored on unsecured personal devices.

4.9 Software Usage and Licensing

- Only legally licensed and approved software may be installed on company systems.
- Unauthorized software downloads or installations are prohibited.
- Software updates and patches must be applied promptly to address known vulnerabilities.

4.10 Physical Security of IT Assets

- Physical access to servers, network equipment, and other critical IT infrastructure will be restricted to authorized personnel.
- Workstations and devices should be secured when unattended.

4.11 Remote Work Security

- Employees working remotely must adhere to all aspects of this policy.
- Secure network connections (e.g., VPN) must be used for accessing company resources from outside the office.
- Home networks and devices used for company work must be adequately secured.

4.12 Security Training and Awareness

- All employees will receive mandatory cybersecurity awareness training upon onboarding and annually thereafter.
- Training will cover key aspects of this policy, common threats, and best practices.

4.13 Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to [HR/ IT Department].
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.
- We also expect our employees to comply with our social media and internet usage policy.

5. TAKE SECURITY SERIOUSLY

Everyone including our customers and partners to our employees and contractors, should feel that their

data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

6. DISCIPLINARY ACTION

We expect all our employees to always follow this policy and those who cause security breaches shall face disciplinary action.

7. DISCLOSURES

The Cyber Security Policy shall be disclosed on the website of the Company i.e. www.dpjewellers.com.

8. POLICY APPROVAL AND REVIEW

The Board will be the approving authority for the Company's overall Risk Management System. The Board will monitor the compliance and approve the Risk Management Policy and any amendments thereto from time to time. This Policy will be reviewed at least once in every two years, including considering the changing industry dynamics and evolving complexity.
