IT Security Policy

Record of Release

Rev No.	Date	Description/Remarks	Prepared By	Reviewed By	Approved By
1.0	01.06.2025	Initial policy	Shailesh Gohil	Dhaval Mankad	

Amendment History

Rev. No.	Date	Nature of Change
1.0	01.06.2025	Initial Document

Shailesh Gohil
Manager – IT

Dhaval Mankad
Vice President - IT

Reference code	Vadilal/IT/2025/02
Effective date	01/06/2025

IT Security Policy

1. **Purpose:**
   - Establish IT security across all endpoints in the network.
   - Ensure effective combination of security products, OS hardening procedures, and end-user awareness.

2. **Applicability**
   - This policy is applicable to Vadilal Industries Limited and Vadilal Enterprise Limited
   - The policy is applicable to all the locations under these companies

3. **Scope:**
   - Covers all endpoints owned by the company: Desktops, Laptops, Workstations, Servers,Networks and Other IT Asset.

4. **Policy Coverage:**

Policy Overview:

- **Security considerations while provisioning of endpoints:**
  - Endpoints must be members of Windows AD domain (VadilalAD.com).
  - Standard OS: Windows 11 Professional.
  - Considering Windows 10 being phased out, all Windows 10 Desktop and Laptop to be upgraded to Windows 11.
  - No users should be configured with admin privileges.
- **Anti-Virus:**
  - Currently we use Trend Micro Vision One XDR
  - Antivirus has protection against Advance Threat Protection, Malware protection, Ransomware protection, Device control i.e USB block, CD/DVD aand Mobile Storage
  - IT System Admin monitors updates and blocks network access upon virus detection.
- **Patch Management:**
  - Currently patches are deployed through Active directory.
  - Periodic OS and security updates from Microsoft are being updated in our network.
  - IT System Admin monitors patch deployment.
- **USB Access:**
  - By default, USB port access on all the devices is disabled.
  - USB port access approval should be taken as per below metrics for respective division. USB port full access approval workflow.
    - VCL – by MD

Shailesh Gohil
Manager – IT

Dhaval Mankad
Vice President - IT

- VIL - Functional Heads (Department Head)
- VIL (Exp, VIU)- Approval of NKG
- VEL – Approval of DLG

- Annual revalidation of USB access to be carried out by taking fresh approval. (Once in a year)
- Currently specific device mapping feature is not available, in future, specific pen drive or external drive will only be enabled which are official.
- If any device (such as a pen drive, mobile device, or USB hard drive) is no longer in use by the user, the user must inform the IT department to have the device access blocked.
-

- **Internet Access:**
  - Default general Internet access has been given to all.
  - If required any Specific site access approval should be taken as per below metrics for respective division. Internet full access approval workflow.
    - VCL – by MD
    - VIL - Functional Heads (Department Head)
    - VIL (Exp, VIU)- Approval of NKG
    - VEL – Approval of DLG

- **Laptop/Desktop/Server Backup:**
  - Currently we are using Druva backup for end points auto backups.
  - We have 330 licenses for Druva backup solution which are allocated based on requirements given by respective department head for key users.
  - For Druva backup we are doing annual verification with department heads for add critical users.
  - Currently we are using Veeam backup solution for Server auto backup.
  - Server Auto backup is schedule after office hours (8 PM).
  - SAP Servers backup are completely managed by SAP Global support team since we are on SAP RISE platform.

- **Password Security/Password guidelines:**
  - Confidentiality of passwords is critical. We have set complex password requirements with Windows Active Directory.
  - Password policy in Windows servers is:
    - Strength is set to Alphanumeric,
    - minimum 8 character and one special character.
    - Password change trigger every 90 days,
    - 5 old password can't be reused
  - Certain system upgradation plans are under implementation post which Windows AD, internet access and email passwords will get unified. (time line Dec2025)

Shailesh Gohil
Manager – IT

Dhaval Mankad
Vice President - IT

- For SAP password, policy is set to
  - 15 characters length ,
  - change every 90 days,
  - last 15 passwords are remembered and can't be reused.

- **Network Security:**
  - Firewalls are implemented in all the office premises to protect corporate networks.
  - Currently SonicWall firewalls are in use.
  - Firewalls are having advance features including Advance Threat protection and intrusion detection/prevention systems (IDS/IPS).
  - All the network switches and firewalls software versions are updated regularly.

- **Network Security (AWS)**
  - For SAP RISE environment, a transit gateway is set-up between our networks and SAP RISE account.
  - Fortinet VPN Firewalls are set-up at Transit Gateway through which remote users can connect to SAP Server.
  - SAP RISE connecting servers or systems are authorized by SAP only to ensure security of entire set-up
  - In addition, AWS account has its own IP access list which is maintained by IT team.

- **Email Security**
  - We are using Trend Micro email security tool to protect corporate email system having feature of Antimalware, Advance Threat Protection, DMARK & DKIM / SPF.
  - Awareness mailers are sent to employees to make them aware on phishing emails.

- **Physical Security**
  - We have implemented physical access controls , Biometric system for critical infrastructure access like server room, Network room and UPS room. Only authorized personnel can access to those rooms.
  - Emergency card access has been provided to security personnel to access those rooms for emergency situations after office hours.
  - Use surveillance systems for monitoring sensitive areas like Serve Room.

- **Server, Network, Software and Application Security Assessment (VAPT)**
  - We are conducting security assessments of critical IT resources yearly.
  - Regularly update and patch software and applications according to VA reports.
  - From April 2025 onwards, VAPT tests are to be conducted at least 2 times in a year.
  - Networking devices: All Network devices will be backed up every month.
  - Core Switches password to be changed every year.

- **Review and Compliance:**

Shailesh Gohil
Manager – IT

Dhaval Mankad
Vice President - IT

- This policy will be subject to periodic review and updates.(One a year)
- Adherence required from all employees to maintain security.

- **Server Operating system and Database security:**
  - All servers must have Windows Server and Database version N-1 (At least one version lower than current version)
  - Any servers/Database not meeting the define policy criteria, must be upgraded within year of this policy.
  - Internet access on server will be disabled unless otherwise required or approved by Head IT.
  - Servers will be patched monthly for critical Windows security or updates.
  - All servers to be backed up on VEEAM backup platform
  - Antivirus – Currently Trend Micro Apex one XDR is installed, getting upgraded to Trend Micro Cloud One Server protect
  - Disable all guest and default Admin accounts on servers.

5. **Effective date and implementation of the policy:**

This policy will be effective from the date of effect mentioned above and overrides all other prevalent policies on this subject.

6. **Exception/Amendments:**

This policy is subject to modification, amendments, and alterations by the management at any time without assigning any reasons or giving any prior intimation. The interpretation of the policy made by the management shall be final and binding on the employees of the company. Any deviations in this policy would need approval from MD/CEO.

Shailesh Gohil
Manager – IT

Dhaval Mankad
Vice President - IT