Itarmi

Laptop & Email Protection Requirements for Engineers

1. Introduction

Compromised engineer laptops are one of the most common causes of:
- Business email compromise (BEC)
- Mass spam being sent from company mailboxes
- Credential theft and lateral movement
- Customer data exposure
- ISO 27001 non-conformities

Engineers are high-value targets because of privileged access and customer interaction.
Security is everyone's responsibility.

2. Mandatory Laptop Security Controls

2.1. Applicability

Applies to: All Itarmi engineers and contractors
Purpose: To prevent mailbox compromise, spam abuse, credential theft, and data loss from engineer laptops.

2.2. Device Protection

Engineers MUST ensure:
- Full disk encryption enabled (FileVault / BitLocker)
- Device protected by strong login password
- Screen lock enabled (max 10 minutes inactivity)
- Local admin rights used only when required
- Automatic OS updates enabled
- Industry standard antivirus / EDR (Endpoint Detection & Response) installed and active
- Firewall enabled

DO NOT:
- Disable security tools
- Share your laptop with others
- Use personal accounts on corporate devices

2.3. Password & Authentication Requirements

Required
- Minimum 14-character password/passphrase
- Unique password per system
- Multi-Factor Authentication (MFA) enabled if possible

Prohibited
- Password reuse across sites
- Storing passwords in browsers or text files
- Sharing credentials via email, Teams, WhatsApp, etc.
- Using customer credentials outside authorised scope

If MFA is available and not enabled — this is a security risk.

3. Email Security – Critical Controls

3.1 Recognising Phishing

Engineers must be vigilant for:
- Unexpected MFA prompts
- "Urgent" payment or credential requests
- Suspicious attachments (ZIP, HTML, ISO, etc.)
- Links that don't match the sender domain
- Messages creating pressure or secrecy

When in doubt:
STOP → VERIFY → REPORT

3.2 Safe Email Behaviour

Always
- Verify external requests for sensitive actions
- Check sender addresses carefully
- Hover over links before clicking
- Report suspicious emails to Itarmi IT
- Use the itarmitech email system only for ITARMI business

Never
- Enter credentials after clicking an email link
- Approve unexpected MFA prompts
- Open attachments from unknown sources
- Auto-forward corporate mail to personal accounts
- Use corporate mailbox for registrations on random websites

3.3 Preventing Spam from Your Mailbox

Mailbox compromise often results in mass spam.

To prevent this:
- MFA should be enabled on email
- Monitor for unusual Sent Items activity
- Use Webmail when possible – if using an App, do not install unknown Outlook add-ins
- Do not grant OAuth consent to unknown apps
- Do not log into email on untrusted machines

If you see emails you did not send — report immediately.

Many modern apps don't ask for your password.
Instead, they ask you to grant permission (consent) to access your mailbox, files, or profile.
This is called OAuth consent

4. Browser & Web Security

4.1 Required Practices

- Keep browser up to date
- Use approved extensions only
- Clear suspicious site permissions
- Block browser password saving
- Use corporate VPN when required

4.2 High-Risk Behaviours to Avoid

DO NOT:

- Download cracked software
- Install random browser extensions
- Bypass certificate warnings
- Use public file-sharing sites for customer data
- Log into itarmitech on public kiosks

5. Network & Remote Working Security

5.1. Public Wi-Fi Rules

When using hotels, airports, cafés:

Always

- Use VPN for corporate access
- Verify network name with venue
- Disable auto-join Wi-Fi
- Keep firewall enabled

Never

- Access sensitive systems without VPN
- Use unknown open networks
- Share hotspot with unknown users

5.2. Home Network Expectations

Engineers working from home should ensure:

- Router firmware up to date
- Strong Wi-Fi password (WPA2/WPA3)
- Default router password changed
- Guest network used where appropriate

6. Software Installation Controls

Engineers must:

- Install software only from trusted sources
- Use Itarmi-approved tools where available
- Remove unused applications
- Keep applications patched

Unauthorised software is a common compromise vector.

7. Data Protection & Handling

Sensitive Data Rules

Always:

- Store customer data in approved locations
- Use encrypted transfer methods
- Follow least-privilege access
- Lock screen when away

Never:

- Store customer data locally long-term
- Use personal cloud storage
- Email large sensitive datasets unencrypted
- Copy customer data to USB without approval

8. Signs Your Laptop or Mailbox May Be Compromised

Report immediately if you notice:

- Emails sent that you didn't send
- MFA prompts you didn't initiate
- Unexpected password reset alerts
- New inbox rules you didn't create
- AV/EDR disabled unexpectedly
- Browser redirects or pop-ups
- Account lockouts
- Unusual login alerts

9. Immediate Actions if You Suspect Compromise

Act fast — time matters.

1. Disconnect from network
2. Do NOT power off unless instructed
3. Change password from a clean device
4. Report to Itarmi Security immediately
5. Do not attempt self-remediation
6. Preserve evidence where possible

10. Engineer Security Checklist (Quick Reference)

Before starting work each day, confirm:

- Laptop fully patched
- AV/EDR running
- VPN available
- MFA working
- No suspicious emails
- No unexpected inbox rules
- Disk encryption enabled
- Screen lock active

11. Compliance & Enforcement

Failure to follow this guidance may result in:

- Security incident investigation
- Access restrictions
- Disciplinary action
- ISO 27001 non-conformity impact

12. Need Help?

Contact:

Itarmi IT: it.helpdesk@itarmi.com

Service Desk: sd@itarmi.com

Escalations: escalations@itarmi.com

Compliance: compliance@itarmi.com