**Employee Security Awareness Guide — Essentials**

Hudson Valley CISO • Updated August 14, 2025

This one-page guide sets expectations for everyday security. Keep it visible; review during onboarding and quarterly refreshers.

# 1) Your Five Golden Rules

• Use strong unique passwords and a company-approved password manager.  
• Turn on MFA everywhere it’s offered.  
• Pause before clicking: verify unexpected links/attachments, even if they look internal.  
• Lock your screen and safeguard devices; report loss or theft immediately.  
• Report anything suspicious right away to security.

# 2) Email and Messaging

Check sender addresses, hover links, and be wary of urgency, gifts, or payment changes. When unsure, use a second channel to verify.

# 3) Devices and Data

Keep systems updated; do not install unapproved software. Store work data only in approved apps. Encrypt sensitive files at rest and in transit.

# 4) Remote Work

Use VPN/SSO when accessing company resources. Avoid public Wi‑Fi without a secure tunnel. Keep family and personal devices separate from work data.

# 5) Reporting

If you clicked a suspicious link, opened an attachment, or see unusual behavior, report it immediately. Early reporting limits damage—no blame.

# 6) Acceptable Use (Summary)

Use company systems for business; protect company data; avoid prohibited content and tools; follow privacy and data handling requirements.