Halberd Capital Partners

Information Security Onboarding Pack - 2026

Document owner: Oluwadamilola (Ola) Adeyemi, Head of IT & Security. Reviewed by Compliance (Anika Shah) 2026-01-09. Replaces the 2025 edition. All new joiners must complete the associated training within 14 calendar days of start date and attest annually thereafter.

1. Welcome

Welcome to Halberd. This pack is your introduction to how we keep our information, our investors' information, and our portfolio companies' information secure. Information security is a firm-wide responsibility; the rules below are the floor, not the ceiling.

If anything in this pack is unclear, send a note to it-help@halberd.com or grab any member of the IT & Security team. Security questions are always welcome, so ask early.

2. Account & Identity

All access to firm systems is mediated by your Halberd identity. Your Halberd identity is issued via the IT onboarding ticket on day one and is governed by single sign-on across the firm's primary applications.

Multi-factor authentication is required for every login. The firm uses hardware security keys (YubiKeys) as the default second factor. Push-based MFA is a fallback only and may not be used for production financial systems.

You will receive two YubiKeys: one primary, one backup. Loss or compromise must be reported to IT immediately. Lost keys may not be replaced more than twice in a rolling 12 months without written sign-off from the Head of IT & Security.

3. Devices

Halberd issues a managed laptop (current standard: 14-inch MacBook Pro with 32GB of memory). All laptops are enrolled in the firm's mobile device management program.

Personal devices may access firm email and calendar via the approved MDM profile. Personal devices may not access firm document repositories, Concur expense, the firm CRM, the data room platform, or any other application classified as Tier-1.

External monitors, peripherals, and adapters are reimbursable up to USD 500 within the first 90 days; subsequent peripherals require IT approval.

4. Email & Communications

Default firm email is hosted on Microsoft 365. External-sender warnings are enabled by default. Encryption is enforced for any message containing financial data, personal data, or deal-specific terms.

Use of personal email for firm business is prohibited. Forwarding firm email to a personal address is a Compliance violation and triggers an automated alert.

Approved messaging platforms: Microsoft Teams (firm-wide), Slack (deal-team channels with Compliance approval), and Signal (encrypted advisor communications, with Compliance approval). WhatsApp may be used only with the firm-issued enterprise client and only for non-substantive logistics (e.g., scheduling).

5. Document Storage

Default document storage is Microsoft OneDrive (personal) and SharePoint (shared). All deal files belong on the deal-team SharePoint site, not on personal OneDrive.

Use of consumer cloud storage (Dropbox personal, Google Drive personal, iCloud) is prohibited for any firm document. Where a counterparty insists on a non-standard data room platform, use the IT-approved guest-access pattern; do not download files to a personal device.

Local laptop storage is encrypted at rest. The firm runs a backup agent that captures local documents continuously; do not assume local storage is durable for original-only files.

6. Network & Wi-Fi

Firm office Wi-Fi (halberd-corp and Halberd-Iot) is segmented. Guest Wi-Fi (halberd-guest) is for visitors only and is internet-only with no access to internal resources.

When working from public Wi-Fi (cafes, hotels, airports), use the firm VPN. The VPN client is preinstalled on issued laptops; the on-demand profile auto-connects on untrusted networks.

Avoid working on highly sensitive deal materials in public spaces; if you must, use a privacy screen and assume your screen is being read by the person behind you.

7. Phishing & Social Engineering

Phishing is the firm's most common security incident category. The firm runs quarterly simulated phishing campaigns. Repeated failures trigger mandatory training.

Common patterns to watch for: payment-instruction changes from a counterparty, urgent wire requests from senior leadership, sham invoice attachments, and fake voicemail-attachment emails. When in doubt, verify out-of-band before acting.

Voice phishing (vishing) and AI-generated voice impersonation are growing risks. If you receive an urgent voice request that is unusual, verify via a second channel before acting regardless of how convincing the voice is.

8. Generative AI Tools

Approved enterprise AI tools: Claude Enterprise, ChatGPT Enterprise, Microsoft Copilot. These deployments are configured to keep data within the firm boundary and not to use firm data for model training.

Use of consumer AI tools (chat.openai.com without enterprise license, claude.ai personal tier, free copilot) for firm business is prohibited.

Outputs from AI tools must be human-reviewed before being relied upon or shared externally. AI-generated content used in client-facing or LP-facing materials must be flagged in the internal review log.

9. Travel Considerations

When traveling internationally, consult the Travel Risk pack on the intranet for any country-specific guidance. Some jurisdictions require travel-specific loaner devices; IT will issue these on request and reset them on return.

Use of public charging cables and untrusted USB ports is prohibited; use your own charger with a power-only adapter or the firm-issued portable battery.

10. Incident Reporting

Any suspected security incident - lost device, suspected phishing click, unauthorized access, leaked credentials - must be reported to security@halberd.com immediately. The on-call responder reviews 24/7.

> *There is no penalty for prompt reporting of an incident, including incidents you may have caused. Late reporting of a known incident is itself an incident and may attract disciplinary action.*

11. Acceptable Use

Halberd systems are firm property and are used only for firm business or limited reasonable personal use. The firm does not actively monitor individual usage for performance purposes but reserves the right to inspect any data on firm systems where lawful and consistent with applicable employment regulation.

Storing or transmitting unlawful, harassing, or discriminatory content on firm systems is prohibited and is a separate disciplinary matter from the underlying conduct.

12. Useful Contacts

- IT Help Desk: it-help@halberd.com
- Security Operations: security@halberd.com
- Head of IT & Security: ola.adeyemi@halberd.com
- Compliance: compliance@halberd.com
- Anonymous Compliance Hotline: see intranet for the third-party-operated reporting line

Appendix A - Glossary

MFA - Multi-Factor Authentication. SSO - Single Sign-On. MDM - Mobile Device Management. VPN - Virtual Private Network. EDR - Endpoint Detection & Response. SOAR - Security Orchestration, Automation & Response. Phishing - fraudulent attempts to obtain credentials or money via email. Vishing - fraudulent attempts via voice. Smishing - fraudulent attempts via SMS.

Appendix B - Day-One Checklist

- Collect issued laptop and YubiKeys from IT.
- Complete SSO setup with Talent and IT.
- Enroll in MDM for any personal devices that need email access.
- Sign electronic acknowledgment of this pack via the LMS.
- Complete the security awareness e-learning module (45 minutes).
- Schedule a 30-minute orientation with a buddy in IT.