ExecAssistants.org

Version 1.0 · July 2026
execassistants.org/resources

Remote EA Security Checklist

For IT Administrators, Operations Leads, and Executive Principals

> Use this checklist to provision secure, auditable access for a remote executive assistant before their first day. Work through each phase in sequence. Share this document with your IT administrator or security lead and with the EA before onboarding begins. Every item in the offboarding section must be completed within 24 hours of an engagement ending, not after.

1 PRE-START IDENTITY SETUP

Days -7 to -3

CORPORATE IDENTITY PROVISIONING

- [ ] Create a dedicated corporate email address for the EA inside your organization's domain. Never allow the EA to use a personal Gmail, Outlook, or shared alias account.
- [ ] Provision the account inside `Google Workspace` or `Microsoft 365 Entra ID` with these settings active:
  - Display name matches the EA's legal or professional name
  - Account flagged as an employee type, not a service account
  - Password policy enforces a minimum 16-character complexity requirement
- [ ] Assign the EA to an EA-specific user group with scoped permissions. Do not add them to a broad admin group to save setup time.
- [ ] Enable mandatory multi-factor authentication (MFA) before the account activates. Hardware token (`YubiKey`) or authenticator app (`Google Authenticator` / `Microsoft Authenticator`) preferred. SMS-based MFA is the least secure option and should be avoided where alternatives exist.
- [ ] Confirm the EA's account is excluded from any shared mailbox or distribution list that grants access beyond their defined operational scope.

PASSWORD VAULT CONFIGURATION

- [ ] Create an EA-specific vault or collection inside your enterprise password manager: `1Password Teams`, `Bitwarden for Business`, or `Keeper Enterprise`.
- [ ] Configure role-based access control (RBAC) so the EA authenticates into designated tools without viewing raw plain-text credentials.
- [ ] Populate the EA's vault with the following access points, set to auto-fill only:
  - Calendar management tools — Calendly, Chili Piper, Motion admin account if applicable
  - Project management platforms — Asana, ClickUp, Notion
  - Communication platforms — Slack, Microsoft Teams
  - Expense and travel tools — Concur, Navan, Expensify
  - Email alias management

- [ ] Remove the EA from any shared credentials that predate the vault setup. Rotate those credentials immediately and re-enter them into the vault so access routes through RBAC from day one.
- [ ] Designate a vault admin, separate from the EA, who can revoke access at any time without involving the EA.

NETWORK ACCESS CONFIGURATION

- [ ] Configure VPN access using `WireGuard` or `IKEv2` protocol for any EA session touching sensitive systems.
- [ ] Choose between split-tunnel and full-tunnel based on your data sensitivity requirements. Full-tunnel is recommended for EAs with access to financial, legal, or board-level systems.
- [ ] Create a dedicated VPN profile for the EA. Do not issue a generic company credential.
- [ ] Test the VPN connection from a non-corporate network before the EA's first day to confirm it functions on a standard home connection.
- [ ] If your organization uses a Zero-Trust Network Access (ZTNA) platform such as `Cloudflare Access`, `Zscaler Private Access`, or `Palo Alto Prisma`, configure an EA-specific access policy that grants access only to the defined tool set.

2 DEVICE AND ACCESS STANDARDS

Days -3 to -1

DEVICE ENROLLMENT

- [ ] Provide a corporate-managed device or enroll the EA's own hardware in your Mobile Device Management (MDM) system before granting any access. Common MDM platforms include `Jamf` (macOS / iOS), `Microsoft Intune` (Windows / Android), and `Kandji`.
- [ ] Confirm full-disk encryption is active: `FileVault` for macOS, `BitLocker` for Windows.
- [ ] Confirm the device runs a current OS and security patches. Devices more than one major OS version behind must not receive access to executive systems.
- [ ] Install and activate endpoint protection software before account activation: `CrowdStrike Falcon`, `SentinelOne`, or `Malwarebytes for Business`.
- [ ] Disable USB mass storage on the EA's managed device to prevent local data exfiltration.
- [ ] Set screen lock to activate after no more than five minutes of idle time.

FILE AND DOCUMENT ACCESS

- [ ] Set all shared documents to cloud-only viewing. Disable the download option inside `Google Drive` or `SharePoint` for any folder containing sensitive materials.
- [ ] Create a dedicated shared folder structure for EA access. Do not grant broad root-level drive access and expect the EA to navigate to what they need.
- [ ] Confirm that no personally identifiable information (PII), financial records, or legal communications sit in folders accessible to the EA beyond what their role requires.
- [ ] If the EA needs access to board documents, isolate those inside a separate workspace or channel with explicit permission grants, not inherited access from a parent folder.

3 DAY ONE ACCESS VERIFICATION

Day 1

SYSTEMS ACCESS WALKTHROUGH

- [ ] Walk through every system the EA will access on day one. Confirm each login works through the vault rather than manually typed credentials.
- [ ] Verify that calendar access grants the correct permission level:
  - **Google Workspace:** set to "Make changes to events" — not "Make changes and manage sharing"
  - **Microsoft 365:** grant "Full Access" only if inbox management is in scope. "Send on Behalf" is a lower-privilege alternative to "Send As" and is preferred where possible
- [ ] Confirm the EA's display name and reply-to address appear correctly in all outbound email. Spot-check before they send any external communications.

COMMUNICATION PLATFORM VERIFICATION

- [ ] Add the EA to relevant `Slack` or `Microsoft Teams` channels within their operational scope only. Do not add them to channels outside their defined role.
- [ ] Confirm the EA appears in the organization directory with the correct name and title so team members can identify them immediately.
- [ ] Confirm the EA accesses `Zoom` or `Google Meet` using their corporate identity, not a personal account.
- [ ] If the EA uses `Loom` for async video briefings, provision a seat under the corporate workspace rather than a personal free account.

FINANCIAL AND EXPENSE ACCESS

- [ ] If the EA submits expenses, add them as a delegate inside `Concur`, `Navan`, or `Expensify` under the executive's account. Do not grant full corporate card admin access.
- [ ] Confirm approval limits clearly in writing. The EA can submit and track expenses. They cannot approve them.
- [ ] If the EA handles travel bookings, confirm they have access to the corporate travel policy and preferred vendor list before making any reservations.

4 ONGOING SECURITY HYGIENE

Monthly and Quarterly

MONTHLY CHECKS

- [ ] Review the EA's active sessions inside your identity provider admin console (Google Workspace Admin or Microsoft Entra ID). Flag any login from an unexpected location or device.
- [ ] Review the EA's vault access log. Confirm they accessed only credentials relevant to their current task scope.
- [ ] Verify that shared document permissions remain at the correct level. Cloud storage permissions drift over time as files get moved, copied, or shared with third parties.
- [ ] Confirm MFA remains active and the EA has not switched to a less secure verification method.

QUARTERLY CHECKS

- [ ] Review the complete list of systems the EA can access. Remove access to any tool no longer active in their role.
- [ ] Rotate sensitive credentials inside the password vault. Update vault entries without sharing new values with the EA directly.
- [ ] Confirm endpoint protection software is current on the EA's device.
- [ ] Run a 30-minute access review directly with the EA. Ask which tools they use daily, weekly, and rarely. Trim access to reflect actual usage, not the original setup scope.
- [ ] Confirm the EA has completed any active security awareness training required of your workforce.

5 REGULATED INDUSTRIES ADDENDUM

Complete if applicable

> Complete this section only if your organization operates in healthcare, financial services, legal services, or another regulated industry. Skip it entirely if none of these apply to your business.

HIPAA — HEALTHCARE

- [ ] Confirm the EA has signed a Business Associate Agreement (BAA) before accessing any system containing Protected Health Information (PHI).
- [ ] Verify that all tools the EA accesses with PHI potential are HIPAA-compliant. `Google Workspace`, `Microsoft 365`, and `Slack` all offer HIPAA-compliant configurations under a signed BAA. Confirm yours is in place before the EA touches any PHI system.
- [ ] Block EA access to PHI via personal devices under any circumstances, including temporary or emergency access requests.

FINANCIAL SERVICES — FINRA AND SEC

- [ ] Confirm that all email and communication systems the EA uses meet your firm's record retention requirements before they send or receive a single message.
- [ ] Route any EA access to trading platforms, client accounts, or portfolio management systems through your compliance-approved access control framework.
- [ ] Log all EA access to financial systems in your firm's audit trail. Do not rely on the EA's own logging.

SOC 2 COMPLIANCE

- [ ] Document the EA's access permissions as part of your formal access control evidence if your organization holds or is pursuing SOC 2 Type II certification.
- [ ] If you used a staffing or outsourcing provider to place the EA, request their SOC 2 compliance documentation for your auditor evidence file.
- [ ] Include the EA's accounts in your next scheduled access review cycle and record the outcome as part of your ongoing SOC 2 evidence.

GDPR — EU CLIENTS OR OPERATIONS

- [ ] If the EA processes personal data belonging to EU data subjects, confirm they understand your organization's data processing obligations before accessing any system.
- [ ] Prohibit local storage of personal data under any circumstances. All processing must occur inside your approved cloud environment.
- [ ] Confirm your Data Processing Agreement (DPA) with every tool the EA uses covers third-party subprocessor access at the EA level.

6 OFFBOARDING PROTOCOL

Complete within 24 hours of engagement ending

> **Critical:** Complete every item in this section within 24 hours of an engagement ending, regardless of how it concluded. Most security incidents involving remote executive assistants occur in the post-termination period, not during the active engagement.

IMMEDIATE ACTIONS — WITHIN 2 HOURS

- [ ] Suspend (do not delete) the EA's corporate identity inside Google Workspace Admin Console or Microsoft Entra ID. Suspension preserves the audit trail for any post-incident review.
- [ ] Revoke all active VPN sessions and remove the EA's VPN profile from the gateway immediately.
- [ ] Remove the EA from the enterprise password vault. Rotate every credential they had access to, including any set to auto-fill only.
- [ ] Revoke calendar delegate access and all mailbox permissions.
- [ ] Remove the EA from all Slack workspaces and Microsoft Teams environments.
- [ ] Check the executive's email account for any forwarding rules routing mail to an external address. Remove any the EA created during the engagement.

WITHIN 24 HOURS

- [ ] Transfer ownership of all Asana projects, ClickUp tasks, Notion pages, and shared documents the EA owned to the appropriate internal team member.
- [ ] Pull and preserve the EA's access logs for the final 30 days before closing the account. Do not delete these records.
- [ ] Remove the EA's endpoint protection profile from your MDM system. Trigger a remote wipe if they used a corporate-issued device, after confirming data recovery is complete.
- [ ] Remove the EA from all Zoom, Loom, Concur, Navan, Expensify, and project management platform accounts.
- [ ] Remove the EA from all active shared inboxes and distribution lists.

WITHIN 72 HOURS

- [ ] Archive the EA's corporate email account in line with your organization's document retention policy. Do not delete it.
- [ ] Complete a final access review and document the full offboarding sequence for your security audit record.
- [ ] Notify any external vendors, partners, or stakeholders who communicated with the EA under the corporate identity that their point of contact has changed.

7 QUICK REFERENCE AND INCIDENT RESPONSE

SECURITY CONTACTS

Complete this table before the EA's first day. Keep it accessible to all relevant parties throughout the engagement.

ROLE	NAME	CONTACT / EMAIL
IT Administrator		
Security Lead		
Password Vault Admin		
MDM Administrator		
Compliance Officer		
EA Primary Contact		
Executive Escalation Contact		

INCIDENT RESPONSE SEQUENCE

> **If you suspect unauthorized access, credential exposure, or suspicious data activity** involving the EA's accounts, act in this sequence immediately. Do not wait for confirmation before starting step one.

1. **Suspend the EA's corporate identity immediately** via your identity provider admin console (Google Workspace Admin or Microsoft Entra ID). Do not wait for confirmation of the incident before taking this action.
2. **Revoke all active sessions and rotate every credential** the EA had access to via the enterprise password vault. Treat all vault credentials as compromised until proven otherwise.
3. **Pull and preserve the EA's access logs** from your identity provider for the preceding 30 days before any account deletion occurs. These records are your primary evidence.
4. **Contact your security lead or IT administrator within one hour** of the suspected incident. Do not attempt to resolve the situation independently or delay notification.
5. **If personal data may have been compromised** and your organization operates under GDPR, the 72-hour supervisory authority notification clock starts when you become aware of the potential breach, not when the breach is confirmed. Start the process now rather than waiting for investigation results.
6. **Document the full incident timeline**, the preserved access logs, and every response action taken with timestamps. Store this record in your security audit file for regulatory compliance and insurance purposes.