Offboarding Checklist

BLACK SWAN
CYBER SECURITY SOLUTIONS

☐ Revoke Access

- **Email Accounts:** Disable or delete email accounts and set up forwarding if necessary.
- **System Logins**: Deactivate all user accounts (e.g., CRM, HR software, financial systems).
- **Physical Access:** Revoke building access (e.g., key cards, codes).
- **VPN/Remote Access:** Disable VPN accounts and remote desktop access.
- **Third-Party Tools:** Remove access to tools like Google Workspace, Microsoft 365, or industry-specific software.

☐ Device Retrieval

- **Hardware:** Collect laptops, mobile devices, USB drives, and other company-owned equipment.
- **Peripherals:** Retrieve company-owned monitors, keyboards, or accessories.
- **Secure Data Transfer:** Ensure no business data is stored on personal devices or external drives.

☐ Data Management

- **Backups:** Securely back up the departing individual's files and emails.
- **Cloud Storage:** Transfer ownership of shared documents and folders.
- **Account Ownership:** Reassign accounts for tools like social media or project management platforms.

☐ Communication and Documentation

- **Internal Announcement:** Notify relevant teams of the departure.
- **External Communication:** Inform clients and partners if the individual had external responsibilities.
- **Exit Interview:** Discuss their departure and remind them of confidentiality agreements.

☐ Security Measures

- **Password Updates:** Change shared passwords for tools the individual accessed.
- **Audit Logs:** Check activity logs for unusual or unauthorized access before or after their notice period.
- **Two-Factor Authentication:** Reassign or reset 2FA devices and tokens.

☐ Compliance

- **Legal Agreements:** Ensure compliance with non-disclosure agreements and return signed confirmations.
- **GDPR/Data Protection:** Confirm that no personal data of the individual or customers is retained unnecessarily.

☐ Training and Knowledge Transfer

- **Handover:** Ensure all projects and responsibilities are handed over.
- **Documentation:** Collect process documentation or notes for future use.

☐ Final Check

- **Audit Access:** Double-check all systems, platforms, and devices for lingering access.
- **Confirm Compliance:** Verify that all steps have been completed and documented.