IGI Cybersecurity

» CYBER DO LIST «

EMPLOYEE ONBOARDING AND OFFBOARDING EDITION

This checklist helps organizations manage cybersecurity for employee onboarding and offboarding. These moments are as critical as day-to-day practices in keeping systems and data protected.

» EMPLOYEE ONBOARDING

Start strong by making cybersecurity part of how you welcome new employees. These steps help set expectations, protect systems, and ensure people only have the access they need.

- [ ] Provide cybersecurity and privacy awareness training as part of orientation
- [ ] Ensure employee reviews and acknowledges the Acceptable Use Policy (AUP)
- [ ] Have employee sign any required confidentiality or NDA documents
- [ ] Assign role-based access with manager approval; provision accounts using least privilege
- [ ] Require user to enroll in multi-factor authentication (MFA) and complete device registration

» EMPLOYEE OFFBOARDING

When someone leaves your organization, cybersecurity needs to be part of the exit process. These actions help close the loop, protect data, and maintain control over access.

- [ ] Disable or revoke all system, application, and physical access immediately upon departure
- [ ] Collect all organizational assets (laptops, mobile devices, keys, ID badges)
- [ ] Plan email forwarding, monitoring, and file ownership transfer after employee departure

» BONUS TIPS

- Maintain a master inventory of employee accounts and assets to simplify transitions
- Review user access periodically to catch lingering or outdated permissions
- Extend onboarding and offboarding practices to contractors, interns, and vendors

Found this helpful? **Download our Cyber Do List** with essential daily, monthly, quarterly, and annual cybersecurity tasks that keep your organization focused and consistent.