IGI Cybersecurity

» CYBER DO LIST «

» DAILY

- [ ] Continuous vulnerability management and device monitoring
- [ ] Make and confirm successful backups
- [ ] Monitor users for abnormal activity
- [ ] Monitor for critical security events

» MONTHLY

- [ ] Conduct and verify patch deployment
- [ ] Provide cybersecurity micro-awareness training
- [ ] Conduct phishing simulation campaigns
- [ ] Generate monthly security metrics/KPIs
- [ ] Validate and update asset inventory
- [ ] Review priority security configurations

» QUARTERLY

- [ ] Review firewall rules and access control lists (ACLs)
- [ ] Test business continuity and disaster recovery plans
- [ ] Update and review risk register
- [ ] User access review
- [ ] Validate role-based access control (RBAC)
- [ ] Validate key security control effectiveness
- [ ] Provide leadership with strategic security program update

AS THEY HAPPEN

These are situational tasks whose frequency may vary:

VENDOR CHANGES

Review third-party vendor risk when adding or modifying vendor relationships

CHANGE MANAGEMENT

Conduct security review for new technologies, applications, projects, or infrastructure changes.

EMPLOYEE ONBOARDING

Provide initial security awareness training, implement RBAC, and provision assets securely.

EMPLOYEE OFFBOARDING

Remove system access, collect organizational assets, etc.

Need guidance? Reach out to your IGI representative or visit IGIcybersecurity.com/contact

» ANNUALLY

- [ ] Conduct annual security awareness training (optional if micro-training is provided monthly)
- [ ] Perform enterprise risk assessment
- [ ] Complete compliance assessments as needed (e.g., ISO 27001, SOC 2, PCI-DSS, HIPAA)
- [ ] Conduct incident response tabletop exercise
- [ ] Perform annual penetration test
- [ ] Adjust security roadmap and submit security budget
- [ ] Review, update, and approve all cybersecurity policies, procedures, and plans