JumpCloud
Directory-as-a-Service

Cybersecurity Due Diligence Checklist

Security isn't one-size-fits-all, and you'll want to tailor your solution to your organization. These are the high impact basics to get you started, though.

CHOOSE RESOURCES TO GUIDE YOUR WORK

- Use the NIST framework.
- Follow the Zero Trust Security methodology.
- Address required regulatory frameworks (PCI, HIPAA, etc.).

IMPLEMENT SECURITY CHECKLIST

- Implement centralized **identity and access management.**
- Require **multi-factor authentication**, wherever possible.
- Implement other **password-management policies**, such as length requirements and secure storage (i.e. one-way hashed and salted).
- Use **SSH keys** to ensure secure server connections.
- Install **anti-virus/anti-malware** mechanisms on machines.
- **Patch** all machines and applications to eliminate security holes.
- Leverage **full-disk encryption**.
- Enforce other **policies** for endpoint control, such as disabling USB access.
- Lock down network access and use **VPNs** to secure traffic.
- Implement **telemetry** and other **monitoring**.

ENSURE ONGOING FORTIFICATION

- Implement an employee training program to share best practices regularly.
- Schedule regular third-party assessments to assess your security posture.