DATA LOSS PREVENTION CHECKLIST

LIGHTEDGE

Your data loss prevention strategy should not only protect against external threats, but also take into account the power your own employees hold to make or break your security posture. Begin structuring your policies from the inside out with the assistance of this expert checklist.

- Classify your data and store it according to your policies.
- Develop and implement an access policy for your physical locations.
- Develop and implement an access policy for your IT infrastructure.
- Monitor data movement within your organization and keep a close eye on what data leaves your organization.
- Know the red flags of an employee at risk of acting against their employer.
- Implement robust endpoint security policies and require multi-factor authentication.
- Educate employees on what internal and external threat actors may do to gain access to your organization's data.
- Enroll in CISA's scanning program to detect vulnerabilities before they can be exploited internally or externally.
- Leverage information on your industry's compliance websites in order to stay on top of security trends.
- Prepare a ransomware protection plan and invest in the appropriate services.
- Don't hesitate to call in reinforcements in the form of managed security services if you cannot meet your data loss prevention goals and objectives.
- Follow the 321 Rule: 3 copies of data, 2 types of storage, and at least 1 in a remote location.

LIGHTEDGE HAD YOU COVERED.

If you're looking to refresh or reinforce your data loss prevention strategy, LightEdge is here to help. Between our managed security services, backups, CaaS offerings, and compliant cloud and colocation options, we are here to give your data loss protection stance the revamp your team and customers deserve. Schedule a call today to learn which solutions are best for your organization.