Data Loss Prevention (DLP) Policy

This Data Loss Prevention (DLP) Policy establishes guidelines for identifying, protecting, and responding to potential data exfiltration and leakage incidents. It supports regulatory compliance and the protection of sensitive data assets.

# 1. Purpose

To prevent unauthorized access, use, or transmission of sensitive data.

# 2. Scope

Applies to all employees, contractors, and systems handling organizational data.

# 3. Data Types Covered

• Personally Identifiable Information (PII)   
• Payment Card Information (PCI)   
• Financial records   
• Intellectual property

# 4. Controls

• Use of email DLP filters and cloud DLP tools   
• USB and external device control   
• Network monitoring for abnormal outbound traffic   
• Encryption enforcement for file transfers

# 5. Incident Response

All DLP alerts must be triaged by the Security Team. Incidents are escalated based on impact level and reviewed quarterly.

# 6. Training and Compliance

DLP awareness training is mandatory annually. Violations may result in disciplinary action.