**LEX RETAIL STORES**

CYBERSECURITY AWARENESS & INCIDENT COMMUNICATION PROGRAM

MONTHLY CYBERSECURITY AWARENESS & PHISHING SIMULATION PROGRAM

NOTE:

All training completions will be tracked and documented.

Employees must digitally sign to acknowledge training completion.

Non-compliance may result in restricted access or disciplinary action.

Objective: To improve cybersecurity culture, reduce risk from social engineering, and increase compliance with internal policies.

**STRUCTURE:**

Frequency: Monthly (1st Monday of each month)

Duration: 1-hour session

Format: 30-minute virtual training + 30-minute phishing simulation debrief

Tooling: Free/open-source platforms like GoPhish, PhishSim, Google Forms for assessments

Month-by-Month Plan:

JAN

Password Hygiene & MFA

Fake password reset email

FEB

Remote Work Best Practices

VPN login notice or device login alert

MAR

Recognizing Phishing & Social Engineering

Fake CEO request for login details

APR

Acceptable Use Policy

Free software/download link

MAY

Protecting Customer Data (PII)

Customer data breach alert

JUN

Secure Use of Cloud Platforms

Google Drive shared file

JUL

Vendor Security Awareness

Fake vendor invoice or payment request

AUG

Email & Messaging Security

Outlook/Slack login notification

SEP

Mobile Device & BYOD Security

SMS-based phishing (smishing)

OCT

Security Incident Reporting

Fake breach disclosure scenario

NOV

Physical Security & Device Locking

USB found in office simulation

DEC

Annual Policy Refresher + Quiz

Review-themed phishing link (bonus quiz)

Evaluation & Reinforcement:

Recognition for phishing simulation top performers

Remedial micro-training for high-risk staff

POLICY ALIGNMENT:

ISO/IEC 27001:2022 A.6.3: Information security awareness, education, and training

ISO/IEC 27001:2022 A.5.1: Policies for information security

ACCEPTABLE USE & REMOTE WORK POLICY TRAINING

Delivery:

Integrated into onboarding and revisited in February & December training sessions

Distributed via internal LMS or secure file sharing

ACCEPTABLE USE

Prohibited activities (torrenting, unauthorized downloads, etc.)

Responsible handling of customer and vendor data

Use of company devices and cloud resources

Zero trust policy

REMOTE WORK ACCESS RULES

Use of Multi Factor Authentication

Use of Virtual Private Network

Use of secure Wi-Fi

ISO Control Mapping:

A.5.1: Management direction for information security

A.6.3: Awareness and training on acceptable usage policies

INCIDENT COMMUNICATION STRATEGY

Objective: Ensure Lex Retail communicates clearly and efficiently during security incidents.

Internal Alert: Notify staff of a suspected breach or phishing incident

Customer Notification: Professional, calm disclosure email if PII is exposed

Vendor Alert: Incident update for external vendors who may be affected

ROLES IN INCIDENT RESPONSE PLAN

|  |  |  |
| --- | --- | --- |
|  | **Role** | **Responsibility** |
|  | CEO: | Final approval of public statement |
|  | IT Lead | Technical investigation & containment |
|  | Customer Support | Respond to customer inquiries |
|  | Legal Advisor | Ensure regulatory compliance |
|  | Communication Officer | Craft and send internal/external updates |
|  | Cybersecurity Officer | Lead incident response and validate system recovery Handle regulatory reporting and customer disclosure |

TABLETOP DRILL SIMULATION

Frequency: Once per quarter

Scenario: Simulate phishing incident leading to credential theft

Outcome: Test IR plan execution and communication flows

RECOVERY PLAYBOOKS & UPDATES

|  |  |
| --- | --- |
| **Phase** | **Description** |
| Containment | Isolate affected systems to prevent spread of malware or data exfiltration. |
| Eradication | Remove malicious files, reset credentials, clean infected devices. |
| Restoration | Recover from backups, reinstall clean images, re-enable services. |
| Validation | Verify system integrity, monitor logs, test user access. |
| Communication | Notify stakeholders, regulators, and customers of restoration progress. |

**COMMUNICATION DURING RECOVERY**

Internal updates every 4–8 hours to execs and department heads

External notifications within 72 hours for customer-impacting breaches

Use pre-approved templates from the communication toolkit

Review Date: August 2026Approved By: Chief Security Officer – Lex Retail Stores

**BACKUP & RESTORATION STRATEGY**

Daily automated backups to encrypted cloud storage

Weekly offline backup to external drives (stored securely)

Quarterly disaster recovery drill simulations

Tested recovery scripts for critical systems

Recovery type: Differential backup system

Recovery Checklists: For cloud app compromise, data leaks, or lost devices

Stakeholder Update Frequency: Internal updates every 24 hours during active incident

External updates within 72 hours where legally required

|  |  |  |  |
| --- | --- | --- | --- |
| System | Priority | RTO/hr | Recovery Method |
| E-commerce Platform | High | 4 | Cloud-based snapshot backup |
| Customer Database | High | 6 | Encrypted DB backups |
| Email & Communications | Medium | 12 | SaaS service restore |
| Internal Admin Portal | Medium | 24 | Restore from VM snapshot |
| Marketing Website | Low | 48 | Static rebuilds or CDN backup |

**POST-RECOVERY ACTIONS**

Root cause analysis (RCA) report within 72 hours

Policy or control updates (e.g., MFA enforcement, access control review)

User re-training for affected teams

Communicate lessons learned to all staff

ISO Control Mapping:

A.5.29: Contact with authorities (regulatory and legal obligations)

A.8.13: Response to information security incidents

BY PRECIOUS