Sterling Oakmont

FINANCIAL SERVICES, LLC

Sterling Oakmont Financial Services — Policy Toolkit

Acceptable Use Policy • Password Policy • Incident Response Plan

Prepared by: Shane Silvernail, M.S. Information Technology (Cybersecurity)

Date: October 2025

Acceptable Use Policy

Purpose

Define appropriate and responsible use of Sterling Oakmont technology resources and ensure the confidentiality, integrity, and availability of company data.

Scope

Applies to all employees, contractors, and third-party users with access to company systems, networks, or data.

Policy

1. **Authorized Use** — Company systems are for legitimate business purposes only.
2. **Access Control** — Users must log in with assigned credentials; sharing accounts is prohibited.
3. **Data Protection** — Sensitive client/company information must not be transmitted outside secure systems or stored on personal devices.
4. **Internet & Email Use** — Internet and email are monitored. Offensive, illegal, or non-business use is not permitted.
5. **Prohibited Activities** — No unauthorized software, attempts to bypass security controls, or activity that may compromise security.
6. **Device Security** — Devices must be password-protected, locked when unattended, and kept up to date.
7. **Reporting Incidents** — Suspected security events must be reported to IT Security immediately.

Enforcement

Violations may result in disciplinary action up to termination and/or legal consequences.

Review

Reviewed annually by IT Security & Compliance or following major system changes.

Password Policy

Purpose

Ensure strong authentication practices safeguarding access to systems and data.

Scope

Applies to all users accessing company networks, systems, or cloud services.

Policy

1. **Complexity** — Minimum **12** characters; include uppercase, lowercase, numbers, and special characters; avoid dictionary words and personal info.
2. **Expiration** — Change every **90 days**; do not reuse the last **5** passwords.
3. **MFA** — Required for remote access, administrative, and privileged accounts.
4. **Storage & Transmission** — Never write down or share passwords; do not send via email or chat.
5. **Service/Shared Accounts** — Managed by IT Security and reviewed quarterly.
6. **Account Lockout** — **5** failed attempts trigger a **15-minute** lockout.
7. **Password Resets** — Identity must be verified per IT procedures.

Enforcement

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

Review

Reviewed semi-annually by the Information Security Officer.

Incident Response Plan (IRP)

Purpose

Define a standardized approach for detecting, responding to, and recovering from cybersecurity incidents.

Scope

Applies to all employees, IT systems, and data assets owned, operated, or managed by the company.

Phases of Incident Response

1. **Preparation** — Maintain updated IR contacts (IT, HR, Legal, Execs); ensure EDR, backups, and logging are active and monitored.
2. **Identification** — Detect via alerts/reports; classify severity (Low/Medium/High/Critical).
3. **Containment** — Isolate affected systems; disable compromised accounts; block malicious IPs/domains.
4. **Eradication** — Remove malware/backdoors; patch vulnerabilities; update firewall rules.
5. **Recovery** — Restore from clean backups; validate integrity before returning to production.
6. **Lessons Learned** — Post-incident review within **5 business days**; document findings and update controls.

Roles & Responsibilities

- **Incident Response Lead** — Coordinates response and communications.
- **IT Security Team** — Executes containment, eradication, and recovery.
- **Management/Legal** — Oversees regulatory and external communications.
- **All Employees** — Report suspected incidents immediately.

Reporting

Report incidents via the IT ticketing system or email **security@sterlingoakmont.com**.

Review

Reviewed annually and after any major incident or infrastructure change.