anj

giving life to ideas!

Standard Operating Procedure (SOP) - Information Security Policy

Document ID: ISP-SOP-003
Effective Date: [29th Jan 2024]
Version: 1.0
Prepared By: Information Technology Department
Approved By: Senior IT Manager – Sagar Pardeshi

---

1. Policy Objective

To protect the organization's information assets from unauthorized access, alteration, loss, or destruction by leveraging **Sophos Firewall** and aligned best practices.

---

2. Firewall & Network Security Policy

- **Perimeter Defence:** All inbound/outbound internet traffic is routed through **Sophos Firewall** for inspection, control, and threat prevention.
- **Segmentation:** DMZ and VLAN segmentation are enforced using firewall rules to isolate critical infrastructure (e.g., servers, databases).
- **Intrusion Prevention System (IPS):** Enabled with auto-updated signatures to block known attacks and exploits.
- **Web Filtering:** Enforced by Sophos Web Protection to block malicious and inappropriate websites based on categories.
- **Application Control:** Non-business-critical applications (e.g., torrents, gaming, P2P) are restricted using Sophos Application Filter.

---

3. Access Control Policy

- **User Authentication:** Sophos integrates with **Active Directory** to enforce user- and group-based access controls.
- **VPN Policy:** Remote users access the network via **SSL VPN or IPsec VPN** with MFA (multi-factor authentication) enabled.
- **Admin Access:** Firewall administration is limited to authorized IT personnel using role-based access and activity logging.

- **Guest Access:** Guest Wi-Fi is isolated and rate-limited through Sophos Wireless Firewall rules.

---

4. Data Protection & DLP

- **SSL/TLS Inspection:** Decryption and inspection of HTTPS traffic are enabled with exclusions for privacy-sensitive apps (e.g., banking).
- **Email Security Integration:** If using **Sophos Email**, policies are aligned to prevent phishing, spoofing, and malware in email communication.

---

5. Update, Patch, and Backup Policy

- **Firmware Updates:** Sophos Firewall is configured for **manual updates after validation** in a staging environment.
- **Backup:** Weekly encrypted configuration backups are scheduled on email.
- **Change Management:** Any change to firewall rules or settings is documented and approved by Senior IT Manager.

---

6. Monitoring and Incident Response

- **Real-Time Monitoring:** Sophos Central collects logs from the firewall for analysis and alerts.
- **Incident Detection:** Alerts are generated for abnormal traffic, failed logins, port scans, or detected malware.
- **Incident Response:** View and action on alerts generated by Sophos firewall.
- **Log Retention:** Logs are stored for at least 6 months as per compliance requirements.

---

7. Audit and Compliance

- **Quarterly Firewall Review:** Firewall rules, IPS signatures, and reports are reviewed quarterly.
- **Policy Compliance:** Internal checks conducted to ensure adherence to this policy.

- **Reports Generated:**
    - Top users by bandwidth
    - Blocked threats
    - VPN usage
    - Web category hits

---

8. User Awareness and Training

- Annual training for employees on safe internet usage, phishing detection, and information handling.
- Specific training for IT staff on Sophos firewall administration and best practices.

---

9. Policy Violation

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination and legal action.

---

10. Review and Approval

- **Owner:** IT Manager
- **Review Cycle:** Annually or upon major firewall/technology changes
- **Approved by:** Senior IT Manager – Sagar Pardeshi

---END---