Standard Operating Procedure (SOP) for Endpoint Security, Secure Access, and Network Perimeter Defense

1. Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish clear guidelines and procedures for the effective management, monitoring, and response pertaining to our organization's endpoint security (Antivirus/EDR), secure remote access (VPN), and network perimeter defense (Firewall). This SOP aims to protect organizational assets, data, and user access from various cyber threats, ensure secure connectivity for remote users, and maintain the integrity and availability of our network services, while ensuring compliance with internal security policies and external regulations.

2. Scope

This SOP applies to all employees, contractors, and third parties involved in the management, monitoring, or direct use of the following systems:

- **Microsoft Defender for Endpoint (MDE):** All endpoints (workstations, servers) covered by our centrally managed MDE deployment.
- **Global Secure Access (GSA):** All users utilizing GSA for secure network access.
- **Sophos Firewall:** The primary network gateway firewall(s) protecting our organizational network.

It covers routine operations, incident response, configuration management, and reporting related to security controls.

3. Definitions and Abbreviations

- **AV:** Antivirus
- **EDR:** Endpoint Detection & Response – Advanced endpoint security that goes beyond traditional AV to detect and investigate suspicious activities.
- **MDE:** Microsoft Defender for Endpoint.

- **VPN:** Virtual Private Network – Creates a secure, encrypted connection over a less secure network, like the internet.
- **GSA:** Global Secure Access – Microsoft's security service providing secure access to internal and cloud resources.
- **Firewall:** A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- **IPS:** Intrusion Prevention System – A network security technology that examines network traffic flows to detect and prevent vulnerability exploits.
- **Gateway:** A network point that acts as an entrance to another network. Our Sophos Firewall serves as the primary network gateway.
- **SOC:** Security Operations Center (if applicable, refers to the team performing security monitoring and response).
- **IOC:** Indicator of Compromise – Forensic evidence of a potential intrusion or attack.
- **False Positive:** A legitimate activity or file incorrectly identified as malicious.
- **False Negative:** A malicious activity or file that was not detected.
- **MFA:** Multi-Factor Authentication.
- **Zero-Trust:** A security model based on the principle of "never trust, always verify."

4. Roles and Responsibilities

- **Chief Technology Officer (CTO):**
    - Overall accountability for endpoint, secure access, and network perimeter security strategy and policy.
    - Approves significant configuration changes, incident response plans, and vendor engagements.
    - Ensures compliance with regulatory requirements.
- **IT Security Team**
    - Weekly monitoring and triage of MDE, GSA, and Sophos Firewall alerts.
    - Investigates and responds to security incidents detected by these systems.
    - Manages MDE policies and configurations.
    - Manages GSA user access, policies, and troubleshooting.
    - Liaises with the Sophos Vendor for firewall rule changes and advanced troubleshooting.
    - Performs regular health checks and maintenance.
    - Generates security reports.

- **Sophos (WorldLink):**
    - Performs advanced troubleshooting and maintenance of the Sophos Firewall appliance/service.
    - Provides expert guidance on Sophos Firewall configuration and security best practices.

7. Procedures

A. Microsoft Defender for Endpoint (MDE) Management

Objective: To maintain optimal endpoint security posture, detect threats, and ensure rapid response using Microsoft Defender for Endpoint.

A.1. MDE Daily/Weekly Monitoring & Alert Review

Frequency: Daily (for critical alerts), Weekly (for comprehensive review and trend analysis).

Steps:

1. **Access Microsoft 365 Defender Portal:** Log in to https://security.microsoft.com/
2. **Review Home Dashboard:**
    a. Check "Active incidents" and "Alerts" widgets for new high-severity items.
    b. Review "Device health" and "Exposure score" trends.
    c. Note any significant changes in "Detections over time" or "Automated investigation status."
3. **Review Incidents & Alerts:**
    a. Navigate to **Incidents & Alerts > Incidents**. Prioritize "High" and "Medium" severity incidents.
    b. For each incident:
        i. Assess the incident graph, affected assets, and associated alerts.
        ii. Determine if Automated Investigation & Remediation (AIR) has completed its tasks.
        iii. Change status to "Resolved" or "Dismissed" if investigation confirms false positive or full remediation.
    c. Navigate to **Incidents & Alerts > Alerts**. Review unassigned or newly generated alerts that are not yet part of an incident. Triage and assign as needed.
4. **Review Device Inventory & Health:**
    a. Navigate to **Endpoints > Device inventory**.

    b. Filter by "Risk Level" or "Exposure Level" to identify vulnerable devices.
    c. Check for devices with "No sensor data," "Inactive," or "Antivirus disabled" status. Initiate corrective action with IT Operations/Helpdesk.
5. **Review Automated Investigations:**
    a. Navigate to **Automated investigations**. Review investigations that are pending or require approval for remediation actions. Approve safe actions.
6. **Review Action Center:**
    a. Navigate to **Action center > Pending actions**. Review and approve any pending remediation actions that require manual approval.
7. **Hunting (Weekly):**
    a. Navigate to **Hunting > Advanced hunting**.
    b. Execute predefined weekly queries to proactively search for suspicious activities or indicators of compromise (IOCs) that might have evaded automated detection.
    c. Investigate any findings.
8. **Document Anomalies:** Record any significant findings, unusual patterns, or critical alerts in the Incident Management System.

A.2. MDE Incident Response & Remediation

Objective: To rapidly contain, investigate, and remediate threats detected on endpoints.

Steps:

1. **Detection & Triage:**
    a. An alert or incident is detected via MDE console, email notification, or user report.
    b. Immediately assess severity and potential impact.
2. **Initial Containment:**
    a. For high-severity alerts on critical assets:
        i. Isolate the device from the network (using MDE's "Isolate device" action).
        ii. Collect investigation package (using MDE's "Collect investigation package" action).
        iii. Run full antivirus scan on the device (using MDE's "Run antivirus scan" action).
3. **Investigation & Analysis:**
    a. Review the incident graph to understand the attack chain, affected processes, and lateral movement attempts.

    b. Examine file details, process trees, network connections, and user activities associated with the alert.
    c. Use Advanced Hunting to search for similar activity across other devices in the environment.
    d. Identify the root cause and full scope of the compromise.
4. **Eradication & Remediation:**
    a. Utilize MDE's remediation actions:
        i. **Stop and Quarantine:** Automatically or manually stop malicious processes and quarantine files.
        ii. **Block Execution:** Add malicious files/hashes to MDE's indicators to prevent future execution.
        iii. **Contain/Isolate:** If not already done, fully contain the threat.
    b. For compromised user accounts, force password resets and review MFA logs.
    c. Clean affected systems of any persistent mechanisms or lingering malware.
5. **Recovery:**
    a. Restore the affected device(s) to normal operation (e.g., remove from isolation).
    b. Verify the endpoint is clean and MDE is fully operational on it.
    c. Ensure data integrity and system functionality.
6. **Post-Incident Activity:**
    a. Document the incident thoroughly in the Incident Management System (including root cause, actions taken, lessons learned).
    b. Update MDE policies, rules, or indicators to prevent recurrence.
    c. If necessary, involve other teams.

A.3. MDE Policy & Configuration Management

Objective: To ensure MDE policies are optimized for detection, prevention, and performance.

Frequency: Quarterly, or as needed for new threats/applications.

Steps:

1. **Review Security Settings (Endpoints -> Configuration management -> Endpoint security policies):**
    a. Review Antivirus policies (scheduled scans, real-time protection, cloud protection level).

    b. Review Attack Surface Reduction (ASR) rules.
    c. Review Exploit Protection settings.
    d. Review Network Protection and Controlled Folder Access.
2. **Manage Exclusions:**
    a. Access **Endpoints -> Rules -> Indicators**.
    b. Review existing exclusions (files, folders, processes) to ensure they are still necessary and not introducing undue risk.
    c. When adding new exclusions:
        i. Ensure a documented justification and approval process is followed.
        ii. Use the most granular exclusion possible (e.g., file hash over folder path).
        iii. Periodically review and remove outdated exclusions.
3. **Manage Custom Detection Rules (Hunting -> Custom detection rules):**
    a. Create or modify Kusto Query Language (KQL) rules to detect specific threats or behaviors not covered by default MDE detections.
    b. Test new rules thoroughly before deployment.
4. **Device Groups:**
    a. Review and update device groups to ensure policies are applied correctly to relevant sets of endpoints (e.g., Servers, Executive Workstations, Test Environment).
5. **Agent Deployment & Updates:**
    a. Ensure MDE agents are deployed consistently across all endpoints.
    b. Monitor agent versions and ensure they are updated to the latest stable release.

A.4. MDE Endpoint Health & Compliance

Objective: To ensure all endpoints are properly onboarded, communicating with MDE, and compliant with security policies.

Frequency: Weekly.

Steps:

1. **Endpoint Communication Check:**
    a. In **Endpoints > Device inventory**, filter for devices with "No sensor data" or long periods of inactivity.
    b. Investigate connectivity issues (e.g., network problems, MDE service stopped).
2. **Antivirus Status Check:**

    a. Verify that antivirus protection is active and up-to-date on all devices.
    b. Investigate and resolve any devices with disabled or outdated AV.
3. **Vulnerability Management (Microsoft Defender Vulnerability Management):**
    a. Access **Vulnerability management**.
    b. Review "Weaknesses" and "Recommendations." Prioritize and track remediation efforts for critical vulnerabilities (e.g., unpatched software, misconfigurations).
4. **Compliance Policy Monitoring (if integrated with Intune/MEM):**
    a. Monitor endpoint compliance status against defined security baselines.
    b. Address non-compliant devices through automated remediation or manual intervention.

A.5. MDE Reporting & Metrics

Objective: To provide insights into endpoint security posture, threat trends, and MDE effectiveness.

Frequency: Weekly.

Steps:

1. **Generate Standard Reports:**
    a. **Threat Report:** Total number of incidents/alerts, breakdown by severity, type (malware, phishing, suspicious activity), and affected devices/users.
    b. **Endpoint Health Report:** Percentage of compliant devices, devices with active AV, sensor status.
    c. **Vulnerability Report:** Top vulnerabilities, remediation progress.
    d. **Automated Investigation Summary:** Success rate of AIR.
2. **Analyze Trends:**
    a. Identify increases or decreases in specific threat types.
    b. Assess the impact of policy changes or security awareness initiatives.
    c. Evaluate the overall effectiveness of MDE.
3. **Distribute Reports:** Share relevant reports with CTO.
4. **Actionable Insights:** Translate report findings into recommendations for improving endpoint security.

B. Global Secure Access (GSA) VPN Management

How to Set Up Global Secure Access (GSA) VPN (Microsoft Entra Private Access)

Important Note: Global Secure Access is an evolving service from Microsoft and some features may still be in preview. Always refer to the latest official Microsoft documentation for the most up-to-date information and best practices.

1. Enable Global Secure Access

First, you need to enable the Global Secure Access feature in your tenant.

1. **Log in to Microsoft Entra admin center:** Go to https://entra.microsoft.com/.
2. **Navigate to Global Secure Access:** In the left-hand navigation pane, expand "Global Secure Access".
3. **Enable:** Go to **Global settings > Remote network management > Onboarding**. Follow the prompts to enable the Global Secure Access service for your tenant. This typically involves selecting the "On" switch.

2. Deploy the Global Secure Access Connector

The GSA Connector is a lightweight agent installed on a Windows Server (or virtual machine) within your on-premises network. It acts as a secure bridge between the GSA cloud service and your internal resources.

1. **Create a Connector Group:**
    a. In "Global Secure Access (preview)," go to **Connect > Connectors**.
    b. Click **"New connector group"**.
    c. Give it a name.
    d. Click "Save."
2. **Download the Connector:**
    a. After creating the group, you'll see an option to **"Download connector service"**.
    b. Download the .exe file.
3. **Install the Connector on a Windows workstation:**
    a. **Dedicated Workstation:** It is highly recommended to install the connector on a dedicated Windows Workstation.
    b. **Network Placement:** The server hosting the connector should have network line-of-sight to the internal resources you defined in your application segments.
    c. **Installation:** Run the downloaded .exe file on the server. Follow the wizard. You will be prompted to sign in with your Global Administrator

credentials. This registers the connector with your Entra ID tenant and associates it with the connector group you created.

d. **High Availability:** For redundancy and load balancing, deploy **at least two connectors** in each connector group.

4. **Verify Connector Status:**
    a. After installation, return to **Connect > Connectors** in the Entra admin center.
    b. Ensure the connector(s) show a "Green" status (Active).

3. Assign Users to Access

Users need to be assigned to the applications you've defined, typically through security groups.

1. **Navigate to Enterprise applications:** In the Microsoft Entra admin center, go to **Identity > Applications > Enterprise applications**.
2. **Find your Application Segments:** You'll see the application segments you created listed as Enterprise applications.
3. **Assign Users/Groups:**
    a. Click on the application segment.
    b. Go to **Users and groups**.
    c. Click **"Add user/group"** and assign the relevant security groups or individual users who should have access to this resource.

4. Configure Conditional Access Policies (Crucial for Security)

Conditional Access policies are essential to enforce Zero Trust principles for GSA access, ensuring only compliant and authenticated users/devices can connect.

1. **Navigate to Conditional Access:** In the Microsoft Entra admin center, go to **Protection > Conditional Access**.
2. **Create a New Policy:** Click **"New policy."**
3. **Name:** Give your policy a descriptive name (e.g., "GSA_PrivateAccess_MFA_CompliantDevice").
4. **Users:**
    a. **Include:** Select the users or groups that will use GSA for private access.
    b. **Exclude (if necessary):** Exclude break-glass accounts.
5. **Target Resources:**

    a. Under "Cloud apps or actions," select **"Global Secure Access (preview) > Private access applications."** (This targets the traffic routed through GSA for your internal resources).
6. **Conditions (Examples):**
    a. **Device platforms:** All device platforms (or specific ones like Windows, macOS).
    b. **Client apps:** Select "Browser" and "Mobile apps and desktop clients" (as GSA client acts as a desktop client).
7. **Grant Controls:**
    a. **Require multi-factor authentication (MFA):** Strongly recommended.
    b. **Require device to be marked as compliant:** If you're using Microsoft Intune for device management, this ensures only healthy, managed devices can connect.
8. **Enable Policy:** Set "Enable policy" to **"On"** (start with "Report-only" mode for testing if unsure).
9. **Create.**

5. Deploy the Global Secure Access Client to Users

Users need a client application on their devices to establish the connection to GSA.

1. **Download Client:**
    a. Users can download the Global Secure Access client from the Microsoft GSA portal (often linked from a user's MyApps portal, or you can provide a direct download link).
    b. **Recommended:** Deploy the client via a modern device management solution like Microsoft Intune or Microsoft Configuration Manager for seamless installation and updates.
2. **User Experience:**
    a. Once installed, the client will automatically attempt to connect to GSA.
    b. Users may be prompted to sign in with their Microsoft Entra ID credentials and complete MFA.
    c. The client creates a local virtual network adapter that routes traffic for the configured private access applications through GSA.

6. Test and Verify

Thorough testing is crucial after setup.

1. **Test from a User Device:**

    a. Have a test user (assigned to the GSA application segments and policies) install the GSA client.
    b. Verify they can successfully connect.
    c. Attempt to access the internal resources defined in your application segments.
2. **Review GSA Traffic Logs:**
    a. In the Microsoft Entra admin center, check **Global Secure Access (preview) > Monitor > Traffic logs** to see successful connections and traffic flow for your defined application segments.
    b. Confirm that traffic from the test user's device to the internal resource is indeed routed through GSA.
3. **Validate Conditional Access:**
    a. Test scenarios that should trigger your Conditional Access policies (e.g., connecting without MFA, from a non-compliant device if that's disallowed).
    b. Verify that access is blocked as expected.

C. Sophos Firewall (Gateway) Management

Objective: To ensure the Sophos Firewall effectively protects the network perimeter and internal segments, with rules managed and reviewed by the vendor.

C.1. Sophos Firewall Daily/Weekly Monitoring

Frequency: Monthly.

Steps:

1. **Access Sophos Central / Firewall Management Console:** Log in to your Sophos management platform.
2. **Review Dashboard:**
    a. Check firewall health (CPU, memory, disk usage).
    b. Review traffic statistics, active connections, and top applications/users.
    c. Note any spikes in denied traffic, dropped packets, or unusual bandwidth usage.
    d. Verify IPS/ATP (Advanced Threat Protection) activity and detections.
3. **Review Alerts & Logs:**
    a. Navigate to **Logs & Reports** section.
    b. Review "System logs" for hardware errors, service failures, or unexpected reboots.

    c. Review "Threat logs" for blocked attacks, suspicious activity, or unusual traffic patterns.
    d. Pay attention to logs related to geo-blocking, botnet detection, and web filtering.
    e. **Note:** Since rules are vendor-managed, focus on understanding what is being blocked and why, rather than direct rule modification.
4. **Traffic Analysis (Monthly):**
    a. Review high-level traffic reports to identify unexpected traffic types, top talkers, or unusual outbound connections that may indicate compromised internal systems.
5. **Document Anomalies:** Record any significant findings or critical alerts in the Incident Management System for follow-up with the ISP

C.2. Sophos Firewall Incident Response & Alert Triage

Objective: To facilitate rapid response to security incidents detected by the Sophos Firewall.

Steps:

1. **Detection & Triage:**
    a. A critical alert is received from the Sophos Firewall.
    b. Immediately assess the nature and potential impact of the alert.
2. **Initial Analysis & Validation:**
    a. Review detailed logs for the alert (source IP, destination IP, port, protocol, rule ID).
    b. Attempt to identify the source and destination devices or users involved.
    c. Determine if the alert is a true positive or a potential false positive.
3. **Communication with Vendor:**
    a. For confirmed or highly suspicious incidents originating from or targeting the firewall, **immediately notify the Sophos Vendor (or managed service provider)** providing all relevant details and logs.
    b. Collaborate with the vendor on containment and eradication strategies.
4. **Internal Containment (if applicable):**
    a. If a compromised internal host is identified, work with IT Security team to isolate the host from the internal network.
    b. If necessary and approved, request the Vendor to temporarily block specific malicious IPs/domains at the perimeter.
5. **Investigation & Remediation (Collaborative with Vendor):**

    a. Work with the Sophos Vendor to determine the root cause, scope, and necessary remediation steps at the firewall level.
    b. Ensure any new threat signatures or blocking rules are applied by the vendor.
6. **Post-Incident Activity:**
    a. Document the incident in the Incident Management System.
    b. Review the incident with the vendor for lessons learned and policy refinement.

C.3. Sophos Firewall Change Management (Vendor-Managed Rules)

Objective: To ensure all firewall rule changes are properly requested, approved, and implemented by the vendor in a controlled manner.

Frequency: As needed (for changes), Bi-annually (for audit).

Steps:

1. **Change Request Submission:**
    a. For any new firewall rule, modification, or removal, the requesting individual must submit a formal Change Request (CR) through the organization's change management system.
    b. The CR must include:
        i. Business justification.
        ii. Source/Destination IPs and ports.
        iii. Protocol.
        iv. Rule lifetime (temporary/permanent).
        v. Risk assessment.
        vi. Requested implementation date.
2. **IT Security Review & Approval:**
    a. The IT Security Team reviews the CR for security implications (e.g., least privilege, potential vulnerabilities, impact on existing security posture).
    b. If approved by CTO for final approval.
3. **Vendor Engagement:**
    a. Upon final internal approval, the IT Security Team communicates the approved CR to the ISP.
    b. Provide all necessary details for rule implementation.
4. **Vendor Implementation & Verification:**
    a. The Sophos Vendor implements the rule change according to the CR.
    b. The vendor provides confirmation of implementation.

    c. IT Security, or the requesting party, performs post-implementation testing to verify the rule functions as expected without unintended side effects.
5. **Change Documentation:**
    a. Update the CR status to "Closed" in the change management system.
    b. Ensure the vendor's documentation of the firewall ruleset is updated.
6. **Rule Audit (Bi-annually):**
    a. Periodically request a full firewall rule export/report from the ISP.
    b. Review all existing rules to ensure they are still necessary, optimal, and adhere to security policies. Remove or modify obsolete rules.

C.4. Sophos Firewall Reporting & Audit

Objective: To assess the firewall's effectiveness and compliance.

Frequency: Quarterly.

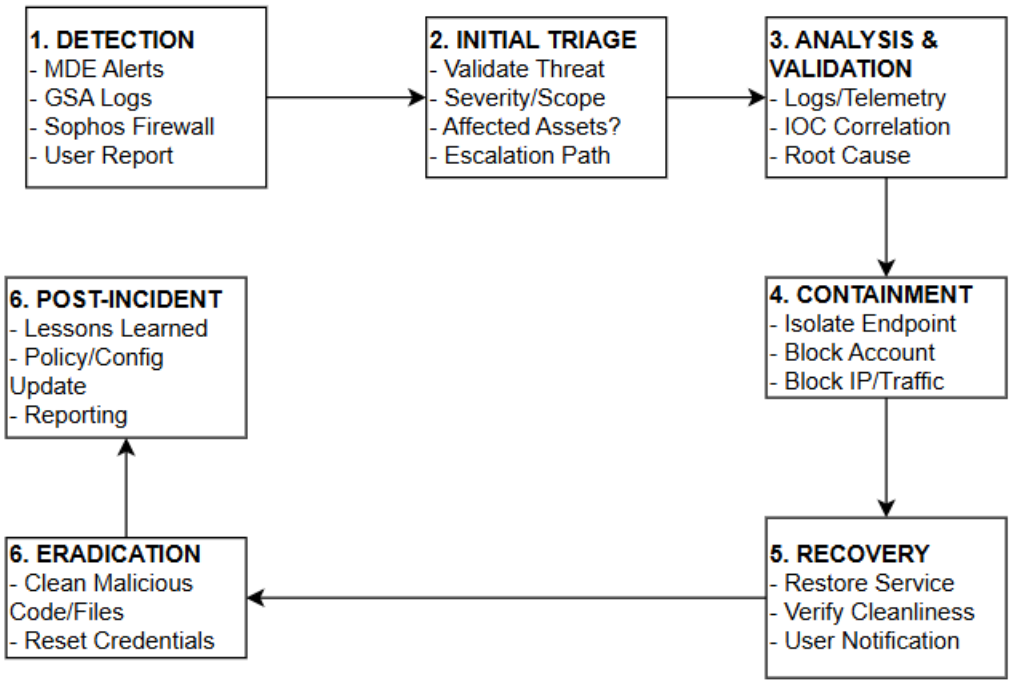
Steps:

1. **Generate Vendor Reports:**
    a. Request monthly/quarterly reports from the Sophos Vendor covering:
        i. Blocked threats (IPS, ATP, web filtering).
        ii. Traffic volume and trends.
        iii. VPN tunnel status and usage.
        iv. Security posture assessment (if provided by vendor).
2. **Review and Analyze:**
    a. Analyze reports for emerging threats, suspicious traffic patterns, or compliance deviations.
    b. Assess the effectiveness of existing firewall policies.
3. **Compliance Audit:**
    a. Verify that firewall configurations and operations align with internal security policies and regulatory requirements.
4. **Distribute Reports:** Share relevant reports with CISO and IT Management.
5. **Actionable Insights:** Translate report findings into recommendations for policy adjustments (to be implemented by vendor) or further security initiatives.

9. Appendix

Appendix A: Security Incident Response Workflow (General)

(Flowchart/Diagram - Conceptual)



Appendix B: Common MDE Alert Categories

- **Malware Detected:** Indication of malicious software on an endpoint.
- **Suspicious Activity Detected:** Behavior-based detection, often pre-malware.
- **Credential Theft Attempt:** Attempts to steal login information.
- **Network Intrusion Detected:** Suspicious network connections or attempts to exploit vulnerabilities.
- **File Activity Detected:** Unusual file modifications, creations, or deletions.
- **Endpoint Health Issues:** MDE agent problems, out-of-date signatures, or real-time protection disabled.
- **Automated Investigation Pending Action:** AIR has completed, but manual approval is needed for remediation.

Appendix D: Sophos Firewall Log Review Locations

- **Log Viewer / Packet Filter Log:** For reviewing allowed/denied connections based on firewall rules. Essential for troubleshooting connectivity or investigating blocks.
- **IPS Log:** Details on detected and blocked intrusion attempts.
- **ATP (Advanced Threat Protection) Log:** Identifies command-and-control (C2) communications and other advanced threats.
- **Web Filter Log:** Shows web access attempts, categories, and blocks.
- **Application Control Log:** Details on applications detected and controlled.
- **VPN Logs (IPsec, SSL VPN):** For monitoring VPN tunnel status, user connections, and troubleshooting.
- **System Logs:** General firewall system events, reboots, service status, hardware alerts.
- **Reports:** Built-in reporting dashboards for traffic, threats, and user activity.