Planet Education Networks

Endpoint Detection and Response (EDR) Policy

Approval Control

Document Title:	Endpoint Detection and Response (EDR) Policy
Approving Body:	Senior Leadership Team ("SLT")
Policy Lead:	IT Manager
Last Review:	September 2025
Effective From:	October 2025
Next Review:	September 2026

Planet Education Networks

Contents

1. Purpose

The purpose of this policy is to establish mandatory requirements for Planet Education Networks' ("PEN") Endpoint Detection and Response (EDR) system to provide comprehensive protection against modern cyber threats including malware, ransomware, and advanced persistent threats, while ensuring compliance with data protection regulations.

2. Scope

This policy applies to all PEN information assets including:

- All PEN-owned workstations, laptops, and servers
- Virtual machines and cloud workloads
- Mobile devices managing institutional data
- All systems connecting to the PEN network via any means
- Contractor devices accessing PEN resources

3. Technical Requirements

3.1. Mandatory EDR Deployment

All in-scope endpoints must have the approved EDR agent installed, actively protecting the system, and communicating with the central management console.

3.2. Configuration Standards

The EDR solution must be configured to:

- Operate in real-time protection mode with continuous monitoring
- Update threat intelligence automatically, multiple times daily
- Perform regular automated scanning according to risk profile
- Enable behavioural analysis and machine learning capabilities
- Implement specific ransomware protection modules
- Maintain full disk encryption enforcement
- Apply application control and execution restrictions

3.3. Monitoring and Analysis

- All endpoint activities must be continuously monitored for suspicious behaviour
- Network traffic must be analysed for malicious communications
- Memory protection must be enabled to detect in-memory attacks
- Cloud-based analytics must be leveraged for threat correlation

4. Roles and Responsibilities

4.1. IT Manager and IT Department

- Manage and maintain the central EDR platform
- Monitor security alerts and conduct threat hunting

- Investigate and respond to security incidents
- Tune detection rules and manage exceptions
- Produce threat intelligence reports for SLT
- Conduct regular security control testing

4.2. IT Support Staff

- Ensure 100% EDR agent deployment and health
- Maintain agent performance and resource optimization
- Remediate compromised or non-compliant endpoints
- Execute containment actions during security incidents
- Maintain deployment and configuration documentation

4.3. All Users

- Must not disable, modify, or interfere with EDR operation
- Must immediately report any system performance issues or security concerns
- Must complete mandatory security awareness training
- Must comply with all endpoint security requirements

4.4. Department Heads

- Ensure staff compliance with endpoint security policies
- Support security initiatives and resource allocation
- Approve business requirements for policy exceptions

5. Incident Response Protocol

5.1. Detection and Alerting

- IT Department must monitor EDR alerts 24/7 via automated notifications
- High-severity alerts must trigger immediate investigation
- All detection events must be logged with full context

5.2. Containment Procedures

- Infected devices must be immediately isolated from the network
- The Security Team will analyse the infection scope and impact
- Compromised systems must be thoroughly cleansed before reconnecting to the network
- Root cause analysis must be performed for all significant incidents

5.3. Recovery and Post-Incident

- Restore affected systems from clean backups where necessary
- Update security controls based on lessons learned
- Document incidents and maintain records for compliance purposes

6. Compliance and Monitoring

6.1. Compliance verification

- Regular audits will be conducted to verify EDR deployment and configuration
- Automated compliance monitoring will alert on non-compliant endpoints

6.2. Policy Enforcement

Devices found to be non-compliant with this policy may be:

- Denied network access until compliance is restored
- Remotely remediated by IT support staff
- Subject to disciplinary action for repeated violations

7. Related Policies and Documents

- Acceptable Use Policy
- Information Security Awareness Policy
- Data Protection and Confidentiality Policy
- Bring Your Own Device (BYOD) Policy
- Password Policy
- Starters and Leavers Checklist

8. Exceptions

Any exception to this policy must be:

- Documented with a business justification
- Reviewed and approved by the IT Manager
- Subject to alternative compensating controls
- Re-reviewed annually for continued necessity