

User Behavior Monitoring & Logs

Prepared By: Muneer Shaukath

Designation: Network Engineer

Version: 1.0

1. Purpose

The purpose of this document is to inform all employees, contractors, and relevant third parties that EFR's monitors user activities on its IT systems to protect information assets, detect potential threats, and comply with legal, regulatory, and contractual obligations.

2. Scope

This monitoring applies to all users accessing EFR networks, systems, devices, and services, including remote and on-site work environments.

3. Systems Used for Monitoring

To ensure effective user activity monitoring and security incident detection, EFR uses the following systems:

- **FortiSIEM:** For centralized log collection, user behaviour analytics, threat detection, and security incident management.
- **ManageEngine Endpoint Central:** For endpoint monitoring, device control, patch management, and compliance tracking.

4. Types of Data Collected

- User login and logout activities
- Access to files, applications, and network resources
- Changes to system configurations
- Internet and email usage
- Installation of unauthorized software
- Connected devices (USBs, peripherals)
- Endpoint security status and compliance

5. Purpose of Monitoring

- Detect and respond to unauthorized or suspicious activities
- Protect company data from breaches, leaks, or misuse
- Ensure compliance with applicable security policies and ISO/IEC 27001 controls
- Support investigations into security incidents or policy violations
- Maintain the integrity and availability of IT systems

6. Privacy Considerations

EFR will ensure that monitoring activities are reasonable, proportionate, and conducted in accordance with applicable data protection and privacy laws. Access to logs is restricted to authorized personnel only, and data is retained securely for defined periods.

7. User Responsibilities

By accessing EFR systems, you acknowledge and consent that your activities may be monitored and logged. Users are responsible for:

- Adhering to all information security and acceptable use policies
- Using company IT resources responsibly and only for authorized purposes
- Reporting any suspected security incidents immediately

For Office Use Only:

Approved By: Sherry George	
Designation: Technical Director	
Reviewed By: Rixon Thomas	
Designation: Sr. Infrastructure Engineer	
Signature Of Approver:	Date:

--End of Document--