**XYZ Telecom Information Security Compliance Policy**

**Version:** 1.0  
**Effective Date:** [Insert Date]  
**Reviewed By:** Chief Information Security Officer (CISO)

**1. Purpose**

This policy outlines the mandatory security compliance requirements for all systems within XYZ Telecom to ensure alignment with corporate security objectives and regulatory obligations. It supports proactive remediation, accountability, and communication between employees, IT support, and security stakeholders.

**2. Scope**

This policy applies to all end-user systems (workstations, laptops, mobile devices) connected to the XYZ Telecom network across all locations in Nigeria.

**3. Security Solutions and Compliance Requirements**

Each system must have the following security solutions installed and functional:

| **Solution Name** | **Type** | **Mandatory Status** |
| --- | --- | --- |
| McAfee | Antivirus | Yes |
| Forcepoint | Data Loss Prevention (DLP) | Yes |
| Lansweeper | Asset Inventory | Yes |
| SolarWinds | Patch Management | Yes |
| BitLocker | System Encryption | Yes |

Systems must be fully compliant with **all five solutions**.

**4. Monitoring and Reporting**

* Security compliance is monitored **daily**.
* Monthly reports will reflect:
  + Total number of assets
  + Compliance % per solution
  + Full vs Partial vs Non-compliant systems
  + Top non-compliant departments, regions, and states
  + National compliance visualized on a geographic map

**5. Non-Compliance Notification Protocol**

When a system is found non-compliant:

**5.1 Notification Message**

* An automated **email and Teams message** will be sent to the user.
* The user's **manager** will be copied.
* Message content will include:
  + Which security solution(s) are missing
  + A **7-day remediation window**
  + Instructions to contact IT Support

**5.2 Escalation**

* If the system remains non-compliant after 7 days:
  + The system may be **blocked and quarantined**.
  + The **line manager’s manager** will be notified.

**5.3 Remediation Confirmation**

* User must click a link to **confirm remediation**.
* Security team will verify system compliance upon confirmation.

**6. Reminder Mechanism**

* Reminder notifications are sent every **48 hours** until:
  + The system is remediated
  + The escalation protocol is triggered

**7. Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| End User | Ensure their system remains compliant |
| IT Support | Assist users in remediation |
| Security Team | Validate remediation and oversee compliance efforts |
| Management | Ensure timely action on escalations |

**8. Policy Enforcement**

Failure to comply with this policy may result in:

* Loss of system/network access
* Formal disciplinary action
* Reporting to executive management

**9. Review and Update**

This policy shall be reviewed **bi-annually** or as required due to changes in tools, threats, or organizational structure.

**Approved By:**  
[Name]  
Chief Information Security Officer (CISO)  
XYZ Telecom

**XYZ Telecom Information Security Compliance Policy**

**Version:** 1.0  
**Effective Date:** [Insert Date]  
**Reviewed By:** Chief Information Security Officer (CISO)

**1. Purpose**

This policy outlines the mandatory security compliance requirements for all systems within XYZ Telecom to ensure alignment with corporate security objectives and regulatory obligations. It supports proactive remediation, accountability, and communication between employees, IT support, and security stakeholders.

**2. Scope**

This policy applies to all end-user systems (workstations, laptops, mobile devices) connected to the XYZ Telecom network across all locations in Nigeria.

**3. Security Solutions and Compliance Requirements**

Each system must have the following security solutions installed and functional:

| **Solution Name** | **Type** | **Mandatory Status** |
| --- | --- | --- |
| McAfee | Antivirus | Yes |
| Forcepoint | Data Loss Prevention (DLP) | Yes |
| Lansweeper | Asset Inventory | Yes |
| SolarWinds | Patch Management | Yes |
| BitLocker | System Encryption | Yes |

Systems must be fully compliant with **all five solutions**.

**4. Monitoring and Reporting**

* Security compliance is monitored **daily**.
* Monthly reports will reflect:
  + Total number of assets
  + Compliance % per solution
  + Full vs Partial vs Non-compliant systems
  + Top non-compliant departments, regions, and states
  + National compliance visualized on a geographic map

**5. Non-Compliance Notification Protocol**

When a system is found non-compliant:

**5.1 Notification Message**

* An automated **email and Teams message** will be sent to the user.
* The user's **manager** will be copied.
* Message content will include:
  + Which security solution(s) are missing
  + A **7-day remediation window**
  + Instructions to contact IT Support

**5.2 Escalation**

* If the system remains non-compliant after 7 days:
  + The system may be **blocked and quarantined**.
  + The **line manager’s manager** will be notified.

**5.3 Remediation Confirmation**

* User must click a link to **confirm remediation**.
* Security team will verify system compliance upon confirmation.

**6. Reminder Mechanism**

* Reminder notifications are sent every **48 hours** until:
  + The system is remediated
  + The escalation protocol is triggered

**7. Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| End User | Ensure their system remains compliant |
| IT Support | Assist users in remediation |
| Security Team | Validate remediation and oversee compliance efforts |
| Management | Ensure timely action on escalations |

**8. Policy Enforcement**

Failure to comply with this policy may result in:

* Loss of system/network access
* Formal disciplinary action
* Reporting to executive management

**9. Review and Update**

This policy shall be reviewed **bi-annually** or as required due to changes in tools, threats, or organizational structure.

**Approved By:**  
[Name]  
Chief Information Security Officer (CISO)  
XYZ Telecom