1. Overview of Information Systems

1. What types of information systems does the IT unit manage?
We manage various systems, including:

- Government intranet services
- Email and document management systems
- Digital media archives
- Internal broadcasting and content distribution systems
- Active Directory and authentication services
- Website and content management platforms

2. What is the primary function of the IT unit within the Ministry of Information?
Our core responsibilities include infrastructure management, network administration, system security, user support, and maintaining the availability and integrity of all ministry-wide digital services.

3. Who are the main users of these systems?
Primarily, ministry staff across departments — including Radio, TV, Newspaper, Admin, and Engineering divisions. Occasionally, external partners use limited-access systems for collaboration.

---

2. Security Policies and Procedures

4. What formal information security policies are currently in use?
Yes, we have documented internal security policies covering acceptable use, password policies, access control, and incident response. These are reviewed annually or when a major system update occurs.

5. How does the IT unit ensure compliance with these security policies?
We conduct periodic staff training and awareness sessions. Compliance is monitored through system logs, endpoint alerts, and spot audits. Violations are addressed with follow-up training or disciplinary measures if necessary.

6. What procedures are followed for securing sensitive or classified information?
Such data is restricted through role-based access control, encrypted during transmission, and stored on secured servers with strict permissions. Classified material is also logged when accessed or modified.

7. Are there any specific regulations or legal frameworks that govern information security for your unit?
Yes, we align with national ICT directives from the Ministry of Transport and Communications, and we are working toward compliance with ISO/IEC 27001 standards.

---

3. Risk Assessment and Management

8. How often does the IT unit conduct risk assessments on its information systems?
At least once a year, or whenever major changes to infrastructure occur. Additionally, informal risk assessments happen during quarterly reviews.

9. What are the most significant security threats identified in your risk assessments?
Top threats include:

- Phishing and social engineering
- Ransomware attacks
- Insider threats from untrained staff
- Legacy systems with outdated firmware

10. What strategies are in use to mitigate these identified risks?
We apply software updates, use antivirus solutions, enforce user awareness campaigns, and isolate legacy systems. We've also recently improved firewall and VPN configurations.

---

4. Technical Security Measures

11. What types of technical security measures are implemented?

- Cisco Firepower firewall and VLAN segmentation
- Antivirus on all endpoints
- Secure Wi-Fi with MAC filtering and WPA2
- Encrypted backups
- Intrusion detection systems (IDS)

12. How is user access to information systems controlled?
Through Active Directory and role-based access control. Password policies and 2FA are applied to critical services.

13. What measures are taken to protect against data breaches?
Real-time monitoring, email filtering, logging, endpoint protection, and user access reviews. In the event of suspected breaches, our incident response protocol is activated.

---

5. Incident Response and Recovery

14. Is there an incident response plan in the MOI?
Yes, established in 2022 and tested semi-annually. The head of the IT Unit oversees execution with support from a designated response team.

15. Can you describe a recent security incident and how it was handled?
A phishing email campaign was detected in 2023 targeting editorial staff. We contained the issue by isolating affected accounts, forcing password resets, and analyzing logs. A security bulletin was later circulated.

---

6. Use of Security Software

- Antivirus and anti-malware (ESET + Windows Defender) are actively running.
- Alerts are triaged by the IT operations team using centralized dashboards.
- All applications are reviewed quarterly for updates and patched accordingly.

---

7. Data Management Practices

- Sensitive data is stored in encrypted volumes (AES-256) and only accessible via secure VPNs or LAN.
- Backups are maintained both on-premises and in cloud-synced repositories.
- Data retention follows a 5-year lifecycle, after which data is securely deleted.

---

8. Incident Response Readiness

- The incident response plan is available digitally and printed in the IT office.
- A log of incidents is maintained in our secure internal SharePoint.
- Tools include network scanners, endpoint scanners, secure VPNs, and a contact list of key responders.

---

9. Staff Behavior and Training

- Staff are routinely trained on security practices and phishing awareness.
- Posters and email bulletins reinforce security measures.
- USB access and printing are restricted unless pre-approved.

---

10. Policy Implementation and Compliance

- Security policies are displayed in the IT office and shared via internal email.
- Staff adherence is monitored by log analysis and access logs.

- Reminders are posted in common areas, particularly regarding password policies.

---

11. Communication and Collaboration

- Security updates are discussed during weekly IT briefings.
- A secure group chat and email thread are used for urgent alerts.
- Staff are encouraged to report incidents via a dedicated internal form or helpdesk ticket.