AL-FARABI KAZAKH NATIONAL UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE
DEPARTMENT OF CYBERSECURITY AND CRYPTOLOGY

LEGAL REGULATION OF INFORMATION SECURITY

Lecturer: PhD, Acting Associate Professor Assem Turarbek

MODULE 2

PUBLIC INSTITUTIONS AND E-GOVERNMENT

LECTURE 8

INFORMATION SECURITY IN STATE BODIES AND E-GOVERNMENT

LECTURE OBJECTIVE

Describe the security function in a public body and explain how documentation, access controls and continuity support e-government services.

LECTURE PLAN

1. Security oversight and documentation

2. Assets, access and continuity

3. E-government portals and gateways

INFORMATION SECURITY OVERSIGHT

Concept or participant	Meaning, duties and application
Security unit	A separate security unit or designated official oversees compliance within the public body.
Scope	Oversight covers documentation, asset and risk management, event registration, audits and continuity.
Separation of duties	The security function reviews how requirements are applied by teams that build and operate systems.

The security function reviews asset management, risk management, lawful software use, event registration and continuity. It also supports internal audit and oversight of external audit. Its organizational separation from development and maintenance gives it a defined role in checking the implementation of requirements by the teams operating the service.

FOUR LEVELS OF SECURITY DOCUMENTATION

Concept or participant	Meaning, duties and application
Level 1	The information security policy sets the organization’s overall rules and responsibilities.
Level 2	Standards and rules cover assets, access, authentication, incidents and other control areas.
Level 3	Procedures describe how staff and technical teams carry out recurring security tasks.
Level 4	Registers and work records provide evidence that staff carried out those tasks.

The documentation levels connect policy with evidence of actual work. A rule about backups is implemented through a recovery procedure, while a backup and restoration log records performance. An audit can then compare the rule, the assigned procedure and the recorded result. Missing evidence makes implementation harder to verify.

ASSETS AND RISK ASSESSMENT

Concept or participant	Meaning, duties and application
Asset inventory	Identify records, services, software, equipment and other resources that support public functions.
Classification	Classify assets according to their sensitivity and operational importance, then assign responsible officials.
Risk assessment	Link threats and weaknesses to the assets they can affect and select a response based on potential impact.

An asset inventory includes the information and the facilities used to process it. Classification and ownership assignments establish who makes protection decisions. Risk assessment considers threats, weaknesses and the effect of disruption. The resulting treatment plan links each action to an asset and a responsible official.

IDENTITY AND STAFF ACCESS

Access by role

Access reflects an employee’s responsibilities and the sensitivity of the resources involved.

Authentication

Multifactor authentication and digital signatures can provide stronger assurance for designated systems.

Departure or transfer

Changes in duties trigger a review of permissions and the return or cancellation of relevant credentials.

Authentication verifies an identity claim, while authorization limits what the account can do. Permissions need review when a person joins, changes duties or leaves. Certificates and other credentials also have a lifecycle. Personnel procedures therefore form part of information security alongside the technical mechanisms used during login.

CONTINUITY AND INCIDENT MANAGEMENT

Incident reporting

Staff follow documented reporting and escalation procedures.

Monitoring and audit

Event records and internal audit help identify gaps and verify whether controls operate.

Redundancy

Backup facilities and redundant processing, storage and communications support service continuity.

Continuity covers the ability to sustain essential public functions and restore interrupted services. Reserve facilities and redundant equipment reduce dependence on a single location or component. Procedures identify priorities and responsible staff. Tests provide evidence that backup resources can support the service and that recovered records remain usable.

E-GOVERNMENT COMPONENTS

Web portal

Provides a single point of access to public information and electronic services.

Integration gateway

Connects e-government systems with other information systems.

Payment gateway

Transmits payment requests and sends payment confirmation to the provider.

Mobile access

A one-time password sent to a registered number can support an eligible service.

The web portal provides the user-facing point of access. The integration gateway enables exchange among systems, and the payment gateway transmits payment requests and results. Banks and other participants connect their systems under the applicable arrangements. One request can therefore depend on several components owned or operated by different parties.

CASE DISCUSSION

An employee moves to another department but retains access to a restricted registry.

Which unit reviews the incident, and which records would show whether the former access was used?

Analysis

The security unit reviews the incident. Role assignments, transfer records, permission changes and access logs show when access persisted and whether it was used. The portal, integration gateway and payment gateway perform separate service functions.

SECURITY DOCUMENTATION IN DAILY WORK

Policy sets the general direction. Detailed rules define access, authentication, mobile media, Internet use and other control areas. Procedures explain how staff implement those rules.

Registers provide evidence of implementation. The lecture lists incident records, server-room visits, vulnerability reports, backup tests and configuration changes as examples.

Security responsibilities arise when an employee joins an organization and receives access. Changes in duties require corresponding permission changes. Staff need to know how to report incidents and protect assigned resources.

Departure procedures address the return of equipment and media, cancellation of access and continuing confidentiality duties. Evidence of these actions supports later review.

CRYPTOGRAPHIC AND AUTHENTICATION CONTROLS

The lecture discusses authentication factors, digital signature certificates and access restrictions for different information categories. The strength of authentication reflects system classification and the risk of unauthorized access.

Credential management includes issuance, use, cancellation and replacement. A technical mechanism remains dependent on clear responsibility for protecting and reviewing the associated credentials.

The source describes reserve server facilities and redundancy in processing, storage and communication channels. These arrangements reduce dependence on a single component or location.

A continuity plan identifies essential functions and recovery priorities. Restoration checks confirm that the recovered service can process requests correctly and that its records remain consistent.

CONCLUSION

1. Public bodies assign an oversight function and document security duties at several levels.

2. Asset classification, identity controls and continuity planning support secure operations.

3. The portal, integration gateway and payment gateway perform separate service functions.

SELF-ASSESSMENT QUESTIONS

1. What is the role of a security function within a public body?
2. How do policies, standards, procedures and operational records relate to one another?
3. Why are asset classification and access reviews important?
4. How do a public service portal, an integration gateway and a payment gateway differ?
5. How does continuity planning support the delivery of electronic public services?

REFERENCES

1. Lecture 8. Information Security in State Bodies and E-Government. Course materials.

2. ISO/IEC 27001:2022. Information security management systems.

3. United Nations. E-Government Survey.