Template for Evidence(s) UI GreenMetric Questionnaire

University : Andijan State Institute of Foreign Languages
Country : Uzbekistan
Web Address : www.adchti.uz

[7] Governance and Digitalization (GD)

[7.14] Compliance with the General Data Protection Regulation (GDPR) or Equivalent National Data Protection Regulations

Institutional Information Security and Data Protection Responsibilities managed through ASIFL Digital Education Technologies and Information Security Units

Responsible unit / position	Data protection or security function	Evidence from institutional duties	Relevant regulation or standard
Digital Education Technologies Center	Institutional digital systems and e-learning oversight	Manages digital education activities, official e-mail services, the institute portal, local network data entry, and electronic learning processes.	Law on Informatization; Law on Electronic Government; O'z DSt 2295:2011; O'z DSt 2863:2014
Information Systems Implementation Department	Information system development and user instructions	Develops requirements, concepts, technical specifications, system documentation, user instructions, launch procedures, and technical support for information systems.	O'z DSt ISO/IEC 12207:2007; electronic document requirements
System Administrator	User access and system security	Registers and removes users, connects/disconnects technical equipment, creates backups, installs software, monitors systems, identifies malfunctions and unauthorized users, and supports users.	Internal regulations; information security policy
Network Management Department	Network, servers, firewall and data center operations	Maintains the national electronic education network connection, telecommunications infrastructure, data center,	Network and information systems standards

		databases, servers, networks, firewall operations, and videoconference equipment.	
Information Security Department	Institutional information security governance	Ensures information security, informs about emerging threats, protects information system resources and databases, analyzes unauthorized actions, and develops security work plans.	RH 45-215:2009; Law on Informatization; Law on Electronic Government
Information Security Network/System Administrators	Vulnerability management and database protection	Assess local/corporate network vulnerabilities, secure network devices, monitor databases/servers/networks, ensure firewall security, protect DBMS environments, and continuously monitor information systems.	Information security regulations and internal procedures

Description:

Andijan State Institute of Foreign Languages (ASIFL) demonstrates compliance with equivalent national data protection and information security requirements through institutional job descriptions, assigned responsible units, and operational procedures within its digital governance structure. As ASIFL is located outside the European Union, GDPR-equivalent compliance is demonstrated through alignment with Uzbekistan's national legislation on education, informatization, electronic government, electronic documents, interactive public services, software life-cycle management, and information security in data transmission networks.

At the governance level, the Digital Education Technologies Center is responsible for the general management of the institute's digital education infrastructure, monitoring of computer technologies, official e-mail services, internet networks, electronic learning systems, copying equipment, and the institute's local network portal. This creates institutional oversight over digital resources and data-related processes used by students, academic staff, administrative staff, and managers. At the system-development level, the Information Systems Implementation Department is responsible for developing requirements, concepts, technical specifications, draft designs, user instructions, launching information systems, and providing technical support. These duties help ensure that institutional information systems are developed, implemented, documented, and supported in a controlled and accountable manner.

At the access-control and security level, system administrators register and remove users, connect and disconnect technical equipment, create system backups, install software, monitor systems, identify malfunctions, maintain information security policy implementation, record installed software and equipment, identify unauthorized users, and provide user support. These measures correspond to core data protection

practices such as access control, system monitoring, secure administration, backup management, and prevention of unauthorized access.

At the network and infrastructure level, network administrators monitor the national electronic education network connection, telecommunications infrastructure, data center operations, databases, servers, networks, firewall activity, and videoconference equipment. These responsibilities support the secure operation of the institute's information infrastructure and reduce risks related to data transmission, network interruption, unauthorized access, and system vulnerability.

At the information security level, the Information Security Department is responsible for ensuring information security, notifying relevant users and units about emerging threats, protecting information system resources and databases, analyzing unauthorized or harmful actions in the information space, developing cooperation in information security, preparing annual and semi-annual work plans, approving staff work plans, and conducting regular internal meetings. The department's network and system administrators also assess vulnerabilities in local and corporate networks, secure network devices and systems, protect databases and DBMS environments, monitor implemented information systems, and take measures to eliminate vulnerabilities.

Taken together, these documented duties show that ASIFL has an institutional framework for data protection and information security based on responsible units, defined roles, access management, system backups, network monitoring, database protection, firewall supervision, vulnerability assessment, user support, and compliance with national digital governance regulations.

Relevant SDGs: SDG 4 (Quality Education), SDG 9 (Industry, Innovation and Infrastructure), SDG 16 (Peace, Justice and Strong Institutions), and SDG 17 (Partnerships for the Goals).

Evidence basis:

- Job descriptions of the Digital Education Technologies Center and its responsible positions.
- Job descriptions of the Information Systems Implementation Department, including system administrator and engineer-programmer duties.
- Job descriptions of the Network Management Department, including network infrastructure, data center, server, database, firewall and videoconference responsibilities.
- Job descriptions of the Information Security Department, including information security governance, threat notification, database protection, vulnerability assessment, and continuous monitoring duties.
- References within the source document to Uzbekistan national legal and technical requirements: Law on Informatization, Law on Electronic Government, O'z DSt 2295:2011, O'z DSt 2863:2014, O'z DSt ISO/IEC 12207:2007, and RH 45-215:2009.

Additional evidence link (i.e., for videos, more images, or other files that are not included in this file):

https://green-institute.adchti.uz/job_duties.php#head-detc

https://green-institute.adchti.uz/

https://green-institute.adchti.uz/#research