İSTANBUL
OKAN ÜNİVERSİTESİ

INFORMATION SECURITY POLICY

Istanbul Okan University considers ensuring the security of information assets belonging to its students, graduates, employees, suppliers, and all stakeholders to be one of the fundamental elements of its institutional responsibility. Our University undertakes to manage information security processes in compliance with legal regulations and national and international standards; to systematically address risks to information assets and protect them in accordance with the principles of confidentiality, integrity, and availability. Within this scope, information security activities are planned, implemented, monitored, and developed through a continuous improvement approach.

Policy Core Actions;

- To ensure information security by safeguarding the confidentiality, integrity, and availability of information assets and personal data belonging to all stakeholders.
- To manage and reduce information security risks by identifying and assessing risks to information assets and bringing them under control through appropriate risk management methods.
- To prevent damage arising from improper use by fulfilling information security obligations in accordance with legal regulations, contractual obligations, and institutional requirements.
- To prevent security breaches by protecting information assets against all internal or external threats, whether intentional or unintentional.
- To ensure information security by implementing the necessary technical and administrative measures against unauthorized access, data loss, and factors threatening information integrity.
- To plan information security measures in a manner that supports business continuity and to ensure operational continuity by minimizing the effects of potential risks.
- To raise awareness and develop an institutional information security culture by communicating information security policies and practices to all employees.

