FAIRLEIGH
DICKINSON
UNIVERSITY

Information Resources and Technology

Data Security Policy on GenAI

Responsible Office:	Office of Information Resources and Technology	
		Effective Date: April 1, 2025
Responsible Official:	Chief Information Security Officer & Chief Information Officer	Last Revision: Last Review:

Generative Artificial Intelligence (GenAI) is a technology capable of generating new text, images, video, and other data by analyzing and modeling existing datasets. This policy ensures that all members of the FDU Community understand that entering information into publicly available GenAI applications may contribute that data to the application's training models, potentially making it accessible beyond the university and exposing confidential information.

Additionally, this policy defines the responsible use and data security requirements for GenAI by University faculty, staff, and students. These requirements supplement existing data security policies established by OIRT. Accordingly, diligence must be maintained to protect the confidentiality, integrity, and availability of Administrative Data and Education Records that may be accessed, processed, or generated through GenAI applications.

A. Confidential, Restricted, or Official Use Only Information must not be entered into any publicly available or commercial GenAI application unless an approved agreement is in place with the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). This agreement must include appropriate data security requirements in compliance with university policies.

B. WISP protect information shall not be entered into any private GenAI application without prior approval from the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). Additionally, if the application is not owned and administered by Fairleigh Dickinson University, an approved use agreement must be executed with the application provider and must include appropriate data security requirements in compliance with university policies.

C. Each GenAI application handling Confidential, Restricted, or Official Use Only Information must have an Acceptable Use Policy (AUP) defining its terms of use, data collection policies, and user responsibilities. Faculty may include the AUP in course syllabi if GenAI is permitted for use in the course.

D. Output from a GenAI application must be reviewed by the submitter of the request for confidentiality, integrity, accuracy, fairness, regulatory compliance, and academic attribution with unintended bias before publication or ingestion into another University system in accordance with current FDU Information Security policies located on https://it.fdu.edu.

E. Confidential, Restricted, or Official Use Only Information must not be retained within GenAI systems after processing, particularly in products and services not hosted by FDU. If the GenAI system allows data deletion, the data must be securely removed once processing is complete unless retention is legally or regulatory required. If deletion is not feasible due to system limitations, alternative measures must be implemented to ensure data confidentiality, such as anonymization or eliminating sensitive data before inputting it into the system.

F. A disclaimer must clearly indicate when GenAI is used to generate data or influence decision-making. This ensures transparency regarding the nature and origin of the information provided.

G. In the event of a suspected or confirmed data security incident involving a GenAI system, users must immediately report the incident to the Data Security Incident Response Team (DSIRT) by contacting the Fairleigh Dickinson University Technical Assistance Center (UTAC) at (973)-443-8822. The UTAC is available 24x7.

Appendix I

Key AI Definitions

- Submitter—End user (student, faculty member, staff) inputting a query or prompt into an AI tool or product
- Generate— the process of creating new content such as text, images, audio, video, or other forms of data based on patterns and information learned from existing datasets
- Generator--A system, tool, or mechanism that creates new content
- Ingestion— the process of inputting, integrating, and processing data into a system

Appendix II

DATA SECURITY INCIDENT RESPONSE TEAM (ROLES AND RESPONSIBILITIES)

The Data Security Incident Response Team membership includes the Chief Operating Officer, the Chief Information Officer, the Chief Information Security Officer, the Chief Academic Officer, the University General Counsel and the University Risk Manager. Each member of the Data Security Incident Response Team (DSIRT) has responsibilities related to the security of all the organization's sensitive information. The DSIRT members listed below have specific responsibilities regarding the reporting and handling of data security incidents. Note that one person may serve in multiple roles.

Senior Vice President and Chief Financial Officer: Frank Barra
Daytime telephones: office: 201-692-2237; Email: fbarra@fdu.edu

Chief Information Officer (CIO): Neal Sturm
Daytime telephones: office: 201-692-8689; Email: sturm@fdu.edu

Chief Information Security Officer (CISO): Kimberley Dawn Dunkerley
Daytime telephones: office: 201-692-7672; Email: ddunkerley@fdu.edu

Privacy Officer: Kimberley Dawn Dunkerley
Daytime telephones: office: 201-692-7672; Email: ddunkerley@fdu.edu

Senior Vice President and University Provost: Benjamin Rifkin
Daytime telephones: Office: 201-692-7093; Email: brifkin@fdu.edu

Office of the General Counsel: Steve Nelson
Daytime telephones: office: 201-692-2466; Email: snelson@fdu.edu

University Risk Manager: Gail Lemaire
Daytime telephones: office: 201-692-7083; Email: lemaire@fdu.edu

Vancouver Campus Executive: Wilfred Zebre
Daytime telephone: office: 604-648-4462; Email: wilfred_zerbe@fdu.edu

Associate Vice President for MIS: Saul Kleinman
Daytime telephone: Office: 201-692-2065; Email: saul@fdu.edu