Data Security Policy

INTRODUCTION

The purpose of this policy is to outline essential roles and responsibilities within the University community for creating and maintaining an environment that safeguards data from threats to personal, professional, and institutional interests and to establish a comprehensive data security program in compliance with applicable law. This policy is also designed to establish processes for ensuring the security and confidentiality of BC's Confidential and Strictly Confidential information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information8o5ccm.e.01 Tc 0.001 Tw 0.229 09 /P <MCID 8 >BD9 -23 TJ0 Tc 0 Tw 2.843

contractors,

service.

Strictly Confidential information includes medical/health information pertaining to members of the University community and data collected in the course of research on human subjects. Strictly Confidential information also includes HIPAA-protected information, export-controlled information, and other sensitive information that the information sponsor or responsible Vice President has determined must remain on a secure BC server.

x Confidential information includes sensitive personal and institutional information. Unauthorized access or modification to personal Confidential information may adversely affect individuals. Unauthorized access or modification to institutional Confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of Boston College.

distributed publication) or is created for a public purpose.

5. The Data Security Committee may from time to time provide clarifications relating to the security classifications, and may, through issuance of Data Security Directives establish more detailed requirements concerning the classification of Information Resources, Information Systems, or specific data.

ROLE OF THE DATA SECURITY WORKING GROUP

1. The University has established the Data Security Working Group to aid in the development of procedures and guidelines concerning the collection, storage, and use of data by the University community, and to assist the Data Security Committee in the implementation of this policy.

2.

commissioning of internal audits and investigations.

- Take actions in response to violations of this policy or any Security Breach.

ROLE OF THE DIRECTOR OF COMPUTR POLICY AND SECURITY

1. The Director of Computer Policy and Security shall, with input from the Data Security Working Group, identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of University data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the Computer System Security Requirements.

2. The Director shall, in conjunction with the Data Security T Cyst Secu the D r

by

post-incident review of events and determine, what, if any changes should be made to University practices or policies to help prevent similar incidents. The Committee shall document the University's actions in response to a Security Breach and its post-incident review in the minutes of the meeting in which the breach is discussed.

ENFORCEMENT SANCTIONS

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result in dismissal from the University.

Approved: William P. Leahy, S.J.
Date: as of 5/14/2024

Boston College Computer System Security Requirements

The University maintains a computer security system that provides at a minimum to the extent technically feasible:

1. Secure user authentication protocols including:
    a) control of user IDs and other identifiers;
    b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
    c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
    d) restricting access to active Users and active User and Td