all College facility users, contractors, suppliers, guests and any other person participating in any College-related activity or attending an event on College premises.

Confidential Data: Data classified as Level 3 (Highly Sensitive) (See Policy Statement 1 for definitions of data classification levels).

Data Administrators: Persons responsible for granting appropriate access to users.

Data Custodians/System Administrators: Individuals responsible for properly storing, protecting, enabling use, and backing up of data and systems. Usually a member of CEIT for on-premises enterprise systems and a vendor for a cloud-hosted solution; may be a combination of CEIT staff and a vendor.

Data/System Users: Persons granted access to institutional data and/or systems in order to perform assigned duties or fulfil assigned roles or functions within an organization.

Data Trustee: Data Accountability Owner, an institutional officer with accountability for, and therefore authority over standards, guidelines and procedures regarding business definitions of data and the access and usage of that data within their authority.

Information Security Framework: An information security framework is a series of documented, agreed and understood policies, procedures, and processes that define how information is managed. Top information security frameworks include ISO 27001, NIST Framework for Improving Critical Infrastructure Security, CIS Critical Security Controls and PCI DSS.

Least Privilege Principle: The principle that individuals (and systems) are granted only those privileges that they need to perform their work tasks and job functions. Privilege includes the ability to perform an action, such as accessing information directly within a system.

Need-to-Know Principle: The principle that individuals (and systems) are provided only with that information they need to know for their work tasks and job functions and at the time they need to know it. While some employees may need to be provided with certain information stored within a system, this need does not mean that they need to be able to access that information within that system by themselves.

System Owner: An individual with respo83o009 T -5.1 (i)-10.8 (s)-10.1 (n)-5.2 .6 (O)1(po)1.85 (t)3.w:

handle Douglas College information assets responsibly within their respective roles and in accordance with this policy.

Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Students in violation of this policy may be subject to disciplinary action under the appropriate policy governing student conduct.

1. The following data classification levels are defined for College data and information:

    a. Level 1 – Public
    Data that is or can be publicly released without causing any harm to the College or a person
    b. Level 2 – Internal
    Data that if released may cause minor harm or embarrassment to the College or a person
    c. Level 3 – Highly Sensitive
    Data that if compromised can cause considerable harm or embarrassment to the College or a person

    (See Data Classification Standard for more information)

2. Access to data and systems should be granted based on "Need to Know" and/or "Least Privilege" principles. Data Trustees and System Owners need to ensure that these principles are followed. If individuals need to access specific information only occasionally, Data Trustees should consider ensuring that the information is provided only when needed, in order to reduce the College's exposure in case an account is compromised.
3. Data/System Users must not access any information they do not need to perform their immediate business responsibilities, regardless of whether this information is accessible to them.

Roles and Responsibilities

have an assigned Data Trustee, and each set of data must have only one Data Trustee, although Data Trustees may appoint Proxies as appropriate.

5. System Owners are accountable for ensuring that systems are assessed for security requirements including those flowing from legislative and contractual obligations. System Owners are also accountable for ensuring that systems are designed, configured, implemented, operated, maintained, upgraded, and decommissioned consistent with the established security standards. All College systems must have an assigned System Owner.

6. System Owners are responsible for ensuring that all systems they are accountable for have an assigned System/Data Custodian(s) and that the custodianship is transferred properly when appropriate.

7. Data/System Custodians (also known as System Administrators) are responsible for configuring the security features of the assets under their administration in accordance with relevant policies, standards, and pr3

E. PROCEDURES

Violations of this policy may constitute a Reportable Activity as defined in the College's Protected Disclosure (Whistleblower) Policy and should be reported in accordance with the procedures found in that policy.

F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, AND RELATED POLICIES

Administration Policies:

- Acceptable Use of Computer and Information Technology
- College Use of Copyrighted Works
- Privacy
- Protected Disclosure (Whistleblower)
- Records and Information Management

Applicable Standards (available on DC Connect for internal users only):

- Data Classification Standard
- Information Security Standards and Guidelines