INFORMATION SECURITY STANDARDS GLOSSARY

A

Administrative Head of Unit is any of the following, or their delegates: Director of a service unit; Head of an academic department; Director of a centre, institute or school; Principal of a college; Dean; Associate Vice President; University Librarian; Registrar; Vice President; Deputy Vice Chancellor & Principal; or President.

Application See ***Software Application.***

Application Server or ***App Server*** is a computer that executes commands requested by a Web Server to fetch data from databases. See also ***Web Server*** and ***Database Server.***

C

CAPWAP (Control and Provisioning of Wireless Access Points) is a secure protocol for managing Wireless Access Points.

CIO Chief Information Officer or delegate.

CISO Chief Information Security Officer or delegate.

Compute Node is a Server configured as a component of a collection (cluster) of Servers that performs jobs delegated to it by scheduling software, not usually intended for direct interactive access by Users. See also ***Server***.

Constituents include internal groups (e.g. faculty, staff and students) and external groups (e.g. the Province of BC, the City of Vancouver, donors, the University Neighbourhoods Association and other community groups).

CVSS (Common Vulnerability Scoring System) is a system used to identify the impact of identified vulnerabilities and assign a priority using a standardized methodology. For more information https://www.first.org/cvss/

D

Database Server is a computer in a network that performs database storage and retrieval. Upon requests from the client machines, it searches the databases for selected records and passes back the results. See also ***Web Server*** and ***Application Server.***

Devices are any computing, data transmission or data storage devices, whether mobile or stationary. See also ***Mobile Devices***, ***Internet of Things (IoT) Devices***, ***UBC-owned Devices*** *and* ***Multi-Factor Authentication Devices***.

Direct Attached Storage (DAS) is digital storage directly attached to the computer accessing it, as opposed to storage accessed over a computer network (i.e. network-attached storage). Examples of DAS include hard drives, solid-state drives, optical disc drives and storage on external drives.

Demilitarized Zone or DMZ is a subnetwork that separates Internet-facing services from internal networks.

E

EMRs (Electronic Medical Records systems) are computerized systems designed to maintain patient data.

ERPs (Enterprise Resource Planning systems) consist of Workday, Salesforce, Human Resources Management System (HRMS), Financial Management System (FMS), Student Information System (SIS), Researcher Information Services (RISe), Graduate Studies Online Application system, Learning Management System (LMS), Campus Wide Login system (CWL), Enterprise Maintenance Management System (EMMS) and the Development & Alumni system.

H

High Risk Information is UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction, e.g. Personal Information and Payment Card Industry (PCI) Information. See also ***Very High Risk Information, Medium Risk Information*** and ***Low Risk Information***.

HTTPS (Hypertext Transfer Protocol Secure) is a communications protocol for secure communication over the Internet and other computer networks.

I

Information Security is the preservation of confidentiality, integrity and availability of UBC Electronic Information.

Information Stewards/Owners are the person(s), or their delegates, who are responsible for determining how UBC Electronic Information may be used and disclosed.

Internet-facing refers to systems or services that are visible or accessible from the Internet.

Internet of Things (IoT) Devices are non-standard computing devices that are network-connected and have the ability to collect, transmit or share data with other devices or systems. IoT Devices are embedded with technology, and can be remotely accessed, monitored and controlled. These devices extend internet connectivity to include any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. IoT Devices only include Mobile Devices, Servers or Workstations when they are connected as a dedicated controller as part of an IoT Device (e.g. medical imaging devices and industrial control systems) and running controlling software such that a non-vendor implemented change in the operating system may impact the usability of the IoT Device. See also ***Remote Access.***

L

LAN (Local Area Network) is a computer network that interconnects computers in a limited area such using network media.

Low Risk Information is UBC Electronic Information that may be freely disclosed. Examples of Low Risk Information include the names and titles of UBC employees. See also ***Very High Risk Information, High Risk Information*** and ***Medium Risk Information***.

M

Malicious Code is any software that is intended to cause undesired effects, security breaches or damage, e.g. attack scripts, viruses, worms, spyware, Trojan horses and logic bombs.

Medium Risk Information is UBC Electronic Information that is not protected by law or industry regulation from unauthorized access, use or destruction, but that nevertheless should be protected because releasing it could cause harm to UBC or others. Examples of Medium Risk Information include plans of UBC facilities, locations of vulnerable research units, financial data, Server/network configurations and copyrighted material. See also ***Very High Risk Information, High Risk Information*** and ***Low Risk Information***.

Merchant Systems are any network component, Server or application that stores, accesses or transmits Payment Card Industry (PCI) Information.

Mobile Devices are any portable computing or data storage devices. These include:

- Laptops (a mobile computer small enough to fit on a user's lap);
- Smartphones, Tablets and PDAs; and
- Mobile Storage Devices/Media (portable devices used to store electronic information, such as USB sticks, portable drives, memory cards, CDs, DVDs).

Multi-Factor Authentication (MFA) is a method of confirming a user's identity in which a user is granted access only after successfully presenting evidence from two or more of the following categories: something they know, something they have or something they are. MFA Devices are one way to enable a secondary challenge during a Multi-Factor Authentication process. See also ***Multi-Factor Authentication Devices***.

Multi-Factor Authentication Devices (MFA Devices) are devices or mechanisms used for Multi-Factor Authentication, including dongles, yubikeys and smartphones with MFA applications.

Mutual Authentication refers to two parties authenticating each other at the same time. In technology terms, it refers to a client or user authenticating themselves to a Server and that Server authenticating itself to the user in such a way that both parties are assured of the others' identity.

P

Payment Card Industry (PCI) Information includes credit card numbers, cardholder names, expiry dates, PINs and service codes.

Penetration Testing, aka pen test, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data. The objective is to find these weaknesses and mitigate them before a hacker does.

Personal Health Information (PHI) means recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual.

Personal Information is recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers. Examples of Personal Information include student names, grades, personal email addresses, home addresses, health information, donor names, prospective employee names and personal banking information.

Personal Use Records are records relating to Users' personal use of UBC Systems, e.g. personal emails, documents, voicemails, text messages, and records of internet and social media use.

Principle of Least Privilege is a security principle that restricts the access privileges of accounts (e.g. program execution privileges, file modification privileges) to the minimum necessary to perform their function.

Privileged Access Management (PAM) is a service used to manage privileged access to systems and services that at a minimum does the following:

- supports compliance with UBC policies and standards for privileged access;
- delegates, controls and filters privileged operations that an administrator can execute based on usage policies;
- automatically randomizes, manages and vaults passwords and other secrets for Privileged Accounts, and doesn't expose them to the administrator except as needed for the minimum amount of time necessary.
- controls access to Privileged Accounts via workflow with check-in and check-out;
- supports Single Sign-on (SSO) for privileged access to Servers to perform administrative tasks;
- minimizes the use of hard-coded passwords by making them available on-demand to applications;
- monitors and records "tamper proof" privileged session activity and creates audit reports;
- sends risk-based alerts when abnormal activity is detected;
- locks down Privileged Accounts at endpoints to prevent lateral movement; and
- detects and suspends suspicious activities using advanced threat analytics.

See also ***Privileged Accounts***.

Privileged Accounts are accounts that provide a significantly greater level of access to a system or application than regular accounts. Privileged Accounts are generally restricted to University IT Support Staff. See also ***User Accounts***.

R

Remote Access is access of UBC Systems from a non-UBC network or location, e.g. home, hotel or café.

S

Server. A Server is a computer that provides data to other computers or other computing devices to support multiple Users. It may serve data to systems on a local

network or across the Internet. Servers include (but are not limited to) ***Application Servers***, ***Database Servers***, ***Web Servers***, ***Compute Nodes*** and ***Storage Clusters***.

Service Providers are vendors, contractors, consultants and other non-UBC employees who provide services to UBC.

SNMP (Simple Network Management Protocol) is a standard protocol for managing devices on the Internet.

Software Application is a piece of software designed to perform a task, typically for end users, such as accounting, human resource management, student information management, and tasks involving artificial intelligence. See also ***Web Application***.

SSH (Secure Shell) is a cryptographic network protocol for securing communications.

SSID (Service Set Identifier) is a name or numerical code used to identify a part of a wireless network.

Storage Cluster is a collection of computers and physical storage devices (hard drives, flash storage, etc.) architected to provide network accessible data storage volumes.

T

Technical Owner is ultimately responsible for providing a system's service/functionality to the campus. Often the Technical Owner is a manager or director. The Technical Owner is responsible for ensuring that operating procedures are developed that meet the policies, information security standards and guidelines as defined by the University.

TLS (Transport Layer Security) is a secure internet communication protocol.

U

UBC Datacentres are facilities at UBC that are designed to house Servers and associated equipment.

UBC Electronic Information is electronic information needed to conduct University Business.

UBC-owned Devices are any Devices that are purchased using UBC funds, including research grants. See also ***Devices***.

UBC Systems are applications, platforms, devices and facilities that are owned, leased or provided by the University, and that are used to store, process or transmit electronic information. These include, but are not limited to:

- computers and computer facilities;
- computing hardware and equipment;
- mobile computing devices such as laptop computers, smartphones and tablet computers;
- Internet of Things (IoT) Devices;
- electronic storage media such as CDs, USB memory sticks and portable hard drives;
- communications gateways and networks;
- email systems;
- telephone and other voice systems; and
- software.

See also ***UBC Electronic Services***.

UBC Electronic Information and Systems includes UBC Electronic Information and UBC Systems.

UBC Electronic Services are an integrated set of components for collecting, storing and/or processing UBC Electronic Information to obtain a desired outcome or deliver a service. They are usually comprised of multiple UBC Systems but can be comprised of a single UBC System. See also ***UBC Systems***.

University Business means activities in support of the administrative, academic and research mandates of the University.

University IT Support Staff are UBC employees or contractors who are responsible for maintaining UBC Systems or assisting Users in the configuration, use, troubleshooting, maintenance and repair of these systems.

Users are faculty, staff, students and any other individuals who use UBC Electronic Information and UBC Systems.

User Accounts are accounts that give Users access to UBC Systems. See also ***Privileged Accounts***.

V

Very High Risk Information is UBC Electronic Information the disclosure of which is very likely to result in harm to individuals. Examples of Very High Risk Information include Social Insurance Number, official government identity card, bank account

information, Personal Health Information (PHI), biometric data, personally identifiable genetic data and date of birth. See also ***High Risk Information, Medium Risk Information*** and ***Low Risk Information***.

VLAN (Virtual Local Area Network) is a part of a local area network that is isolated from other parts of the network.

W

Web Application is a Software Application that is stored on a remote Server and delivered over the Internet through a browser interface. See also ***Software Application***.

Web Server is a computer system that hosts websites. It runs software, such as Apache or Microsoft IIS, which provides access to hosted webpages over the Internet. See also ***Database Server*** and ***Application Server.***

Workstations are desktop or laptop computers used for University Business.