

# 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**.

**Core Systems** consist of the Human Resources Management System (HRMS), the Financial Management information System (FMS), the Student Information System (SIS), the Researcher Information Services (RISe), the Graduate Studies Online Application system, the Learning Management System (LMS), the Campus Wide Login system (CWL) and the Development & Alumni system.

**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 or data storage devices, whether mobile or stationary. See also **Mobile Devices**, **UBC-owned Devices** and **Multi-Factor Authentication Devices**.

**DMZ or Demilitarized Zone** 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.

## 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.

**IoT (Internet of Things) Device** is a physical object that is connected to the network with an IP address, and may collect or share data with other devices or systems.

## 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:

1. **Laptops** (a mobile computer small enough to fit on a user's lap);
2. **Smartphones, Tablets and PDAs**; and
3. **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 two or more pieces of

evidence. Evidence falls into the categories of 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 (MFA) Devices***

***Multi-Factor Authentication (MFA) Devices*** are devices 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 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.

***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***.

## 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 Node*** and ***Storage Cluster***.

**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 for end users, such as accounting, human resource management, and student information management. 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

**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 services, 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:

1. computers and computer facilities;
2. computing hardware and equipment;
3. mobile computing devices such as laptop computers, smartphones, and tablet computers;
4. electronic storage media such as CDs, USB memory sticks, and portable hard drives;

5. communications gateways and networks;
6. email systems;
7. telephone and other voice systems; and
8. software.

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

**Work Remotely** means accessing UBC Electronic Information from outside of a UBC campus.

**Workstations** are desktop or laptop computers used for **University Business**.