Information Security Office (ISO)
Glossary of Terms & Iconography

Glossary of Terms

-A-

Administrator Access is defined as a level of access above that of a standard end-user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. Under most circumstances this level of access is relegated to privileged accounts. The following are examples of administrator access:

- In a traditional Microsoft Windows environment, members of the Power Users, Local Administrators, Domain Administrators and Enterprise Administrators groups would all be considered to have Administrator Access.
- In a traditional UNIX or Linux environment, users with root level access or the ability to *sudo* would be considered to have Administrator Access.
- In an application environment, users with elevated privileges, 'super-user', system or database administrator roles and responsibilities would be considered to have Administrator Access.
- Network and other infrastructure systems administrators are also considered to have Administrator Access.

-B-

-C-

Controls are technical, administrative, or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting, or lessening the ability of a particular threat from negatively impacting business processes. Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are implemented.

Control Objectives are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a control, which is what a Standard is intended to address. Where applicable, Control Objectives are directly linked to an industry-recognized secure practice to align cybersecurity and privacy with accepted practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny.

-D-

Dark Web is a hidden part of the Internet that is not accessible from traditional web browsers such as Google Chrome, Safari, Internet Explorer, Firefox, etc. The Dark Web is estimated to be close to 90% of the overall Internet. Many illicit activities are known to take place on this part of the Internet including drug trafficking, illegal weapons trade, prostitution, terrorism, etc.

Data Custodian is university personnel or designated third-party agent responsible for the operation and management of information systems which collect, manage, process, or provide access to University Data. See University Information Asset Classification & Management Policy for roles and responsibilities of Data Custodians.

-E-

Endpoint/Endpoint device is an electronic computing device that connects to a network and communicates back and forth with that network. Endpoints include desktop computers, laptop computers, tablets, mobile devices, or any similar network enabled device.

-F-

-G-

Guidelines are recommendations which can be customized and used in the creation of procedures or to help explain policies and standards.

-H-

-I-

IP Address is an identifier, based on the Internet Protocol (IP) standard (RFC-791), for computer systems and devices connected to the campus network.

-J-

-K-

-L-

Local Access refers to all connections to a University resource performed directly through the system console or console serial connection.

-M-

MAC Address or Media Access Control address, sometimes referred to as a hardware or physical address, is a unique, 12-character alphanumeric attribute that is used to identify individual electronic devices on a network.

-N-

Network-based Access refers to all connections to a University resource performed via a network (e.g., University wired or wireless network, remote networks).

-O-

-P-

Privileged Account is a user account that has more privileges than ordinary users. Privileged accounts might, for example, be able to install or remove software, upgrade the operating system, or modify

network, system, application, or database configurations. They might also have access to files that are not normally accessible to standard users.

Policy defines the security objectives and the security framework of the UO.

Procedure is a detailed step by step how-to document that specifies the exact action which will be necessary to implement important security mechanisms.

-Q-

-R-

Registered and configured for ISO ongoing vulnerability scans means that the ISO can conduct vulnerability scans against the device as is necessary for compliance, security, or policy reasons.

Resource Administrator – *this may variously refer to a service administrator, system administrator, database administrator, network administrator, or device/endpoint administrator depending on the resource in context. I.e., a* ***resource administrator*** *is the person who is responsible for, configures or administrates, a system, device, application, or service.*

-S-

Server is any device which provides service to other network devices regardless of the scale of those services.

Service Provider *– is a unit or person who provides Resource Administrator's functions to a collection of information systems resources.*

Standard is a mandatory action that gives formal policies support and direction.

Standard End-User Access is defined as a user whose access is limited to specific areas necessary to perform their job duties. These users do not, normally, perform *A*dministrator Access duties or are labeled as privileged user accounts.

System, Application, and Service can be loosely defined as any electronic environment that stores, processes or transmits information for the purpose of maintaining the operational functions of University.

-T-

Top-level Administrator or their designee is the head of the college, department, or unit (e.g., Vice Provost/Vice President/Dean/Department Head).

TOR Network (https://www.torproject.org/about/overview.html.en) is the most common mechanism used to access "Dark Web" resources; it provides anonymity to users.

Two-factor Authentication (a.k.a., Two-Step Login, 2FA) is defined as a second layer of security to protect an account or system. Users must go through two layers of security before being granted access to an account or system. The University of Oregon provides a Two-Step Login service that uses DUO Security to manage the second factor authentication.

-U-

University computing and information resources are a collection of systems, applications and services that are in the custody of the University.

-V-

Vulnerability Scanning is an automated, high-level test that looks for and reports potential known vulnerabilities.

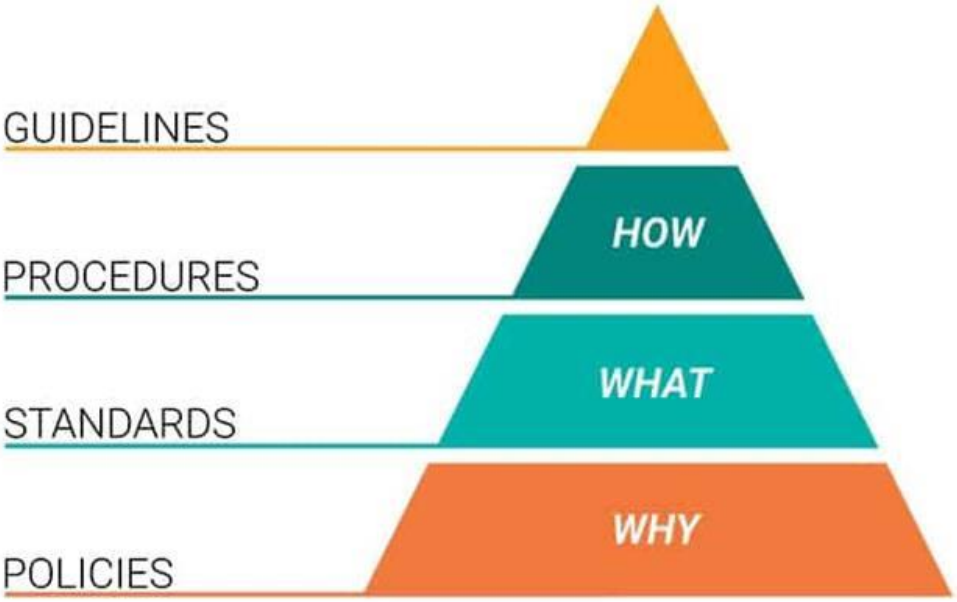
-W-

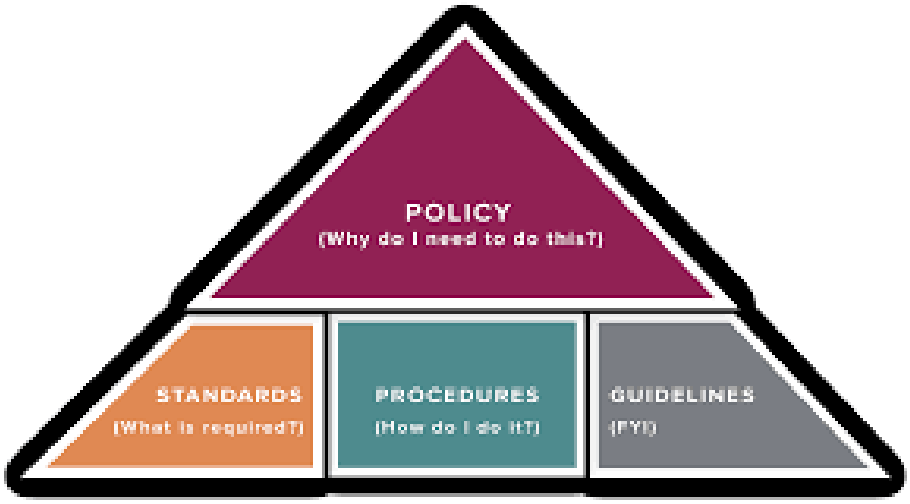
-X-

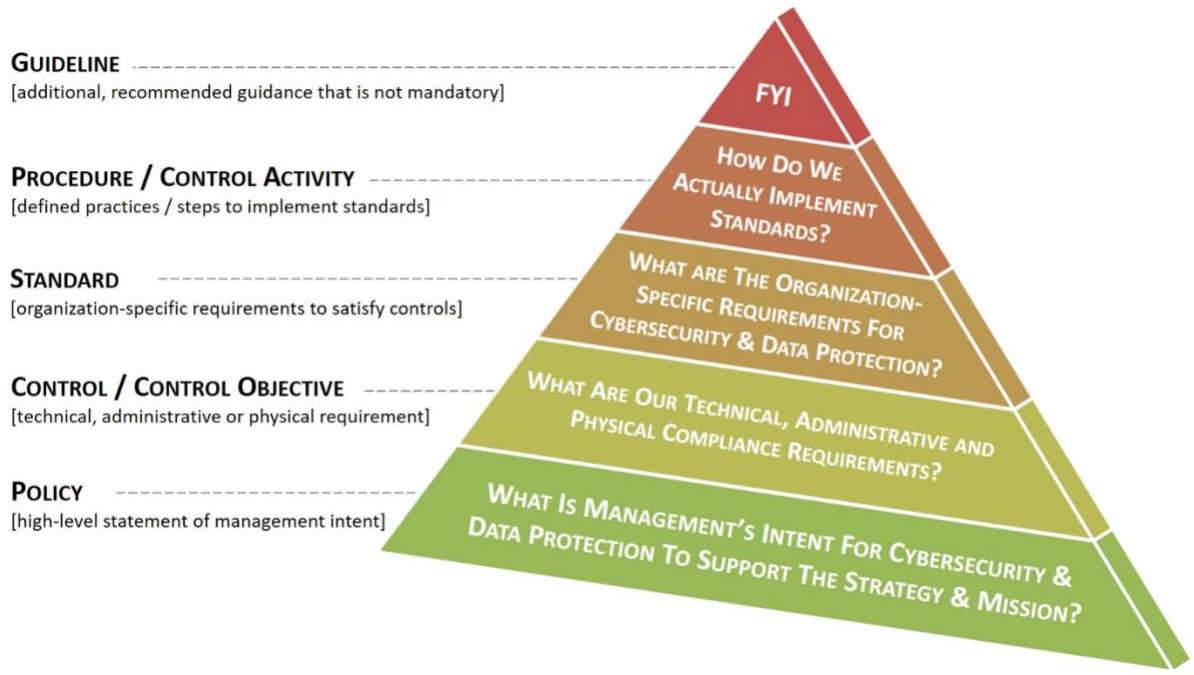
-Y-

-Z-

Iconography







Revision History

Version	Published	Author	Description
1.0	08/09/2022	Information Security Office (ISO)	Original publication

Status:	Published
Published:	**08/09/2022**
Last Reviewed:	**08/09/2022**
Last Updated:	**08/09/2022**