Definitions

Sensitive data - Information of a confidential or proprietary nature as well as other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy. Sensitive information includes but is not limited to information such as medical and health records, grades and other enrollment information, credit card, bank account and other financial information, social security numbers, personal addresses, phone numbers, etc.

Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

IP address - An address assigned to accomplish routing on the Internet.

Domain Name System (DNS) – The method or scheme for assigning names within an IP address.

Address Space – defines a range of discrete addresses, each of which may correspond to a physical or virtual memory register, a network host, peripheral device, disk sector or other logical or physical entity. The Internet Assigned Numbers Authority (IANA) [1] allocates ranges of numbers to various registries in order to enable them to each manage their particular address space.

Sub domain - a domain that is part of a larger domain

Domain Name – a unique name that identifies an Internet site; On the Web, the domain name is the part of the Uniform Resource Identifier (URI) that tells a domain name server where to forward a request for a web page.

IP Address - a unique string of numbers that identifies a computer or server on the Internet. These numbers are normally shown in four groups separated by periods.

VLAN - The acronym VLAN expands to Virtual Local Area Network. A VLAN is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.

DHCP – Dynamic Host Configuration Protocol (see: RFC2131).

Server - For purposes of this policy, a Server is defined as an internal Lawrence Technological University Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

Firewall - A hardware and software device that controls access between two networks. There are several different mechanisms for performing this access control but the essential point is that a firewall implements a network security policy.

Restricted Data - Information protected because of protective statutes, policies, or regulations. This level also represents information that isn’t by default protected by law, but for which the information owner has exercised their right to restrict access.

VPN (Virtual Private Networking) – A mechanism that encrypts the traffic between the VPN Server and the remote computer and allows the remote computer to obtain an onsite IP address.
**Production Network** - the network used in the daily business of Lawrence Technological University and whose impairment would result in direct loss of functionality to Lawrence Technological University employees or students, or impact their ability to do work.

**SNMP** - an application layer protocol that facilitates the exchange of management information between network devices; this is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

**Remote User** - Any user of IT Resources from an off-campus location