



# POLICY MANUAL

## INFORMATION TECHNOLOGY

---

**Number 550**

**Subject: Appropriate Use of Computing, Networking, and Information Resources**

**Effective Date: February 1, 2008**

---

### 550.1 PURPOSE

This policy is intended to be consistent with Utah State University's established culture of academic freedom, intellectual curiosity, openness, and integrity by defining the requirements and limits of appropriate use of information technology resources and services including computers, digital networks, and information resources at Utah State University. These rules are in place to protect faculty, staff, students, and the University. Inappropriate use exposes Utah State University to risks including compromise of network systems and services, loss of confidential data, loss of the resource for legitimate use, and legal liability.

### 550.2 DEFINITIONS

- Authentication credentials – userID/PIN, username/passcode or other secrets or keys used to gain access to a restricted Resource.
- Capacity of Resource – some Resources have a limit that can be exceeded by certain uses, either causing the Resource to crash or causing unacceptable delays in the delivery of results.
- Malware – programs that “infect” computers to do things the user doesn't want or even know about – often giving control of the computer to outsiders or reporting to outsiders the private information sent from or stored on the computer.
- Phishing – messages and/or websites that impersonate legitimate businesses (especially banks) in order to intercept authentication credentials for individuals.
- Privilege – while access is generally granted to everyone in a relevant role, the right is retained by the University to revoke that access when it is in the interest of the University, such as to protect the Resource from use in violation of policy or use in excess of capacity.

- Resource – Computing, Networking and Information Resources – including end-user computers such as desktops, laptops, PDAs, smartphones, Blackberries, Treos; servers; peripherals such as printers, scanners, webcams; firewalls; network routers; wireless access points (see USU Policy 552 [Wireless Deployment](#)); databases; enterprise information system; system of record; shadow systems; etc.
- Restricted Resources – some Resources are available only to individuals in particular roles while other Resources (USU homepage, for instance) are available without restriction and without authentication by the user.
- Role – a category of user who is given access to a particular restricted Resource; may be as general as faculty or student, or as specific as advisor or auditor.
- Strong Password – a password that is not easily guessed by individual or automated guessing, and is not easily cracked by hackers. Strong passwords are generally long and are not composed of words, names, numeric sequences or keyboard patterns. Some central services automatically impose a strong password requirement; but many desktop systems leave this good practice to the user.
- User – faculty, staff, students, and guests of the University.

### **550.3 POLICY**

USU Computing, Networking and Information Resources are provided as a service for use by faculty, staff, students, and guests in a responsible manner that is within the capacity of the Resource and consistent with the mission of the University.

Authentication credentials (e.g., ID/password) are assigned as an access privilege for restricted Resources that may be relevant to the role of the user as faculty, staff, student, or visitor. Users must maintain a strong password. Credentials must be protected from use by anyone other than the assigned individuals. Credentials may be revoked to protect the Resources.

Users of Resources must obey relevant federal, state, and local laws with special attention to intellectual property laws (copyright), communications laws (libel, harassment, obscenity, child pornography, privacy, etc.), and government property laws (non-commercial use, etc.). The University will cooperate with law enforcement agencies when allegations of violation are made.

Users of Resources must protect the integrity of the Resource and the confidentiality of stored and transmitted data by following directions specific to the Resource being used and the data being accessed. Those directions will be provided by IT or other administrators of the Resource or data. This requirement guards against “social engineering” attempts by outsiders to mislead users in ways that allow the outsider to gain access to the Resource or data (e.g., viruses, phishing, hidden malware, etc.).

User-owned equipment connected to the University network must be properly registered and managed in compliance with the separate USU Policy 551 [Computer Management](#) to protect against technical vulnerabilities which will allow outsiders to gain access to the Resource or data.

University-owned equipment must comply with USU Policy 551 [Computer Management](#), however users of that equipment should be alert for any indication of deficiencies in compliance that may result in compromise to the security of the Resource or data.

Users are expected to recognize that the Resources being provided are subject to compromise and other failure at any time in spite of professional efforts in compliance with industry best practices.

Users should take extra precaution to protect their own privacy, to insure the confidentiality of their own personal identifying information, and to guard against the loss or destruction of their own intellectual property as a result of any compromise or failure.

While the University respects the user's privacy, information stored on or transmitted through the Resource is subject to exposure by technical, legal, and extra-legal means beyond the control of the University.

USU Information Technology is directed to interpret this policy and other relevant University policies as they apply to the changing deployment of Resources and provide [Appropriate Use Procedures and Standards](#) that specify in greater detail the required, recommended or prohibited uses of specific Resources. Those procedures and standards will clarify, but not limit or change, the scope of approved policies; and will be approved by the IT Users Advisory Committee.

#### **550.4 ENFORCEMENT AUTHORITY & PENALTIES**

Disciplinary action or sanctions for violations of this policy will be in accordance with USU Policy 311 [Disciplinary Procedures](#) for exempt and non-exempt employees, USU Policy 407 [Academic Due Process: Sanctions and Hearing Procedures](#) for faculty, and [Article VI](#) of the Student Code for students.

---

[BACK TO TABLE OF CONTENTS](#)

<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------