1.430 COMPUTING RESOURCES & ACCEPTABLE USES

1.430.02 Acceptable Use – Generally *(11.4.4)*

A. Employees will comply with **TU 10-01.02 Acceptable Use Policy** as it pertains to the acceptable use of university owned or authorized information resources.
   1. Information resources includes all university-owned computers, applications, software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; classroom technologies; communication services and devices, including electronic mail, voice mail, modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.
   2. University information resources are designed and intended to conduct official agency business. Exceptions to business related uses include, but are not limited to:
      a. Personal use that is infrequent and limited in scope and duration so that employees are not unnecessarily distracted from the faithful and diligent performance of their assigned duties. See also **1.314 Attention to Duty**; and
      b. Professional and career development purposes when in keeping with the provisions of this directive and with prior supervisory approval.

B. In addition to the requirements of the TU Acceptable Use Policy, employees will:
   1. Take reasonable and prudent precautions to prevent the introduction of viruses, malware, or other corrupting software into agency information resources;
   2. Not knowingly install or uninstall, or cause to be installed or uninstalled any hardware, software or peripheral equipment on university information resources without going through the agency's in-house administrative privilege representative to the Office of Technology Services (OTS);
   3. Take steps to prohibit unauthorized access to information resources by:
      a. Logging off any secure network at the end of their tours of duty or after they are finished accessing these networks remotely;
      b. Locking their computers or logging out when they are temporarily away from their on-campus or remote-access computers that are connected to secure networks or applications;
   4. Use only those computers on which they are currently logged in or with direct permission of the primary user;
   5. Guard against the loss of data stored within the agency's information resources;
   6. Report problems with various information resources to the appropriate designated officials or departments.

1.430.04 Data Stewardship

Employees will comply with **TU 10-04.00 Data Stewardship Policy** as it pertains to managing, accessing, and using data in a manner that is consistent with the university and agency's need for data security and confidentiality.

1.430.06 User Names & Passwords *(82.1.6.c)*

A. The university's computing network and the agency's CAD/RMS both automatically require that users change their passwords at least every 90 days to verify access permissions and security.
B. Employees will change their passwords as required to ensure they maintain actively accessible accounts in the university's network and, if required, in the agency's CAD/RMS system.

1.430.07 SECURITY UPDATES

THE OFFICE OF TECHNOLOGY SERVICES REGULARLY AND AUTOMATICALLY UPDATES AND PATCHES ALL OPERATING SYSTEM AND APPLICATION SECURITY VULNERABILITIES FOR ALL COMPUTERS AND SERVERS ON THE UNIVERSITY NETWORK. SEE ALSO **TOWSON UNIVERSITY'S POLICY ON SECURITY UPDATES.**

1.430.08 Electronic Record Storage

A. To ensure the integrity of departmental information and continuity of departmental work products, employees will ensure that all original, official, and agency related electronic work products are stored within their university-provided **"Home"** drives **(H:\)** or, if directed to do so, on the departmental "Organization" drive **(O:\)** rather than on the hard drives **(C:\)** of any personal or departmental desk-top or lap-top computers. These work products include, but are not limited to files created in Microsoft Word, Excel, PowerPoint, Picture Manager, etc.
B. Employees may choose to make and retain local or working copies of their departmental work products on local hard drives **(C:\)** or other media, such as flash drives or rewritable CDs, but will ensure that:
   1. Personal identification information or confidential work products are not stored on any portable media because the media may be lost or stolen; and
   2. Originals are updated as soon as reasonably possible after being modified and working copies are deleted.

1.430.10 Email

A. The agency uses the university provided and maintained email system as an official communications tool and a primary means of facilitating official agency communications and actions.
B. Agency correspondence conducted via email carries the same effect and importance as hard copy correspondence.
C. Emails must conform to the same professional, ethical, and lawful standards as hard copy correspondence.
D. Secondary purposes of the agency's email network are to encourage and facilitate intra-agency communications.
E. All employees, except for those assigned to duties out of the agency's immediate service area, are responsible for viewing any new departmentally related emails at least once each tour of duty.

1.430.12 Social Media

A. The agency endorses the use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. Listing individual social media types, brand names, etc. is impractical because of the still emerging nature of these communications platforms.
B. The agency's official social media presence is limited only by the agency's resourcefulness to lawfully use these various tools.
C. Any public, official presence in social media by the agency:
   1. Must be approved by the Chief or designee and overseen by a commander specified by the Chief;
   2. Be clearly marked as maintained by the agency, with contact information clearly displayed, and state that any posted comment is subject to public disclosure;
   3. Will conform to all applicable directives;
   4. State that any opinions posed by visitors do not necessarily represent the agency's opinion and that posted comments will be monitored with the agency maintaining the right to remove obscenities, off-topic comments, personal attacks, and other inappropriate content.
D. Employees who participate in the agency's public, official social media presence will:
   1. Clearly identify themselves as agency employees;
   2. Conduct themselves at all times as representatives of the agency and consistent with applicable directives; and
   3. Release only approved content and information. See also **2.0429 Public Information**.
E. The agency's use of the internet and social media platforms to investigate criminal activities and to collect criminal and homeland security intelligence is limited to only those lawful activities approved by the Chief or designee and overseen by a commander specifically designated by the Chief.
   1. Investigative social media accounts will not be used for personal use.

2. Officers conducting investigations using internet or social media resources will do so only while working on-duty and in an official capacity.
    a. Investigating officers will not access or download any items that are illegal while using personal computers on their home networks, internet café, or other non-departmental internet access points.
    b. Social media accounts or websites that contain, upload, download or present any type of digital information pertaining to child pornography, exploitation of children, terrorist activities, sales of illegal drugs or other sensitive crime will be accessed only by authorized officers assigned to specific investigations using specifically designated computers.

F. Employees who choose to maintain or participate in personal social media activities:
1. Should be aware that disseminated information is not necessarily private or protected and may be relevant in criminal, civil, and administrative proceedings;
2. Will conduct these activities lawfully, ethically, consistent with any applicable university and agency directives, and in ways that are not unbecoming of employees;
3. Will not disseminate any information to which they have access solely as a result of employment with this agency unless the information has already been officially released to the public or permission has been granted by the Chief or a designee;
4. Will not disseminate images of agency logos, patches, uniforms, vehicles, or similar identifying images unless permission has been granted by the Chief or a designee; and
5. May identify themselves as employees of the agency and thereby be held responsible and accountable for representing the agency positively and professionally in their social media activities.