## PURPOSE:

To assure the confidentiality, integrity, and availability of CSU Channel Islands information assets by regularly assessing the University’s network and information systems for vulnerabilities.

## BACKGROUND:

The University is required by CSU systemwide policy to protect its information assets. An industry best practice in information security is the regular assessment of the computing environment for security vulnerabilities. T&C will scan the University network, including non-University-owned hardware connected to the network, on a regular basis.

## BUSINESS PRACTICE:

### Accountability:

The Chief Information Officer.

### Applicability:

All users of networked information resources at CSU Channel Islands, the Security Incident Response Team, and T&C system administrators.

### Text:

In order to ensure the confidentiality, integrity, and availability of the University’s information assets, T&C will implement the following procedures.

***Address space scans***

Channel Islands T&C operates one or more address space scanning appliances. T&C will regularly scan the entirety of the University’s address space to create and maintain an inventory of connected devices. These scans are non-invasive and will not affect properly configured systems.

For purposes of this business practice, “University’s address space” includes—

1. All internal Internet Protocol (IP) addresses, including those address spaces allocated to University auxiliaries and departments, and those addresses allocated to University wireless networks, and
2. All externally-facing Demilitarized Zone (DMZ) IP addresses assigned to the Channel Islands campus.

These scans will retain the following information about devices discovered for use by T&C personnel in the performance of their duties:

1. The date and time of the device’s discovery,
2. The IP address of the connected device,
3. The Media Access Control (MAC) address of the connected device, along with the mapping of the MAC address to the device’s manufacturer,
4. A list of open Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP) ports on the device, and
5. The scanning device’s best guess as to the device’s operating system.

***System vulnerability scans***

Certain systems operated by T&C contain information or provide services critical to the University’s operation. These systems will be periodically scanned for software vulnerabilities. Channel Islands T&C operates one or more vulnerability scanning appliances for this purpose.

Vulnerability scanning is a more intrusive process than address space scanning and will only be applied to a University-owned system with notice given to the administrator.

Automated regular vulnerability scans will not be applied to non-University-owned systems connected to the University network.

***Incident vulnerability scans***

In the event of a threatened, suspected, or actual security event or incident, Channel Islands T&C may employ a vulnerability scan against any device connected to the University network. A reasonable effort, commensurate with the severity of the ongoing incident, will be made to contact the owner or administrator of the system being scanned.

***Reviewing scan results***

Channel Islands T&C will periodically review the results of address space scans. This information will be used to assess demographic information about the University’s computing environment, such as the types and kinds of devices being operated on the University network. This information will also be used to note changes to the computing environment. The information may also be used in response to an incident for containment or forensic purposes.

Channel Islands T&C Security Incident Response Team (SIRT) will review the results of system vulnerability scans on a bi-monthly basis. The information will be used to assess and mitigate security risks on the scanned systems.