Disablement of Enterprise Technological Security Controls

Fairfield University	**POLICY AND PROCEDURES**

POLICY ON Disablement of Enterprise Technological Security Controls

Fairfield University's Information Technology Services (ITS) organization implements industry standard technological security controls across our institution to minimize financial damages, legal liability, theft or destruction of Fairfield University's data, damage to Fairfield University's physical infrastructure, and interruptions of Fairfield University's software systems.
These enterprise technological security controls include but are not limited to firewalls, mail security appliances, network access control systems, and endpoint protection suites such as anti-virus programs.
Organizations outside of ITS may identify circumstances where these enterprise technological security controls are preventing the execution of Fairfield University business processes.
The following circumstances are examples of requests to disable enterprise technological security controls:

- Disabling blocks to known-malicious websites.
- Allowing email ("whitelisting") from known-malicious sources.
- Disabling routine scanning of network traffic or email.
- Disabling registration requirements to access the Fairfield University wireless network.
- Disabling or uninstalling anti-virus across the enterprise.

Requests to disable enterprise technological security controls must be approved by either the Chief Information Officer (CIO) or the Executive Vice President (EVP).
The following circumstances are routine requests and do not constitute a request to disable enterprise technological security controls:

- Disabling blocks to a website which has been shown to be non-malicious.
- Allowing email ("whitelisting") from a non-malicious source.
- Manually registering individual devices to the Fairfield University wireless network.
- Disabling or uninstalling anti-virus on an individual device to allow compatibility with specific software suites.

Routine requests that do not constitute disablement of enterprise technological security controls do not require special approval.

PROCEDURE

Approved requests to disable enterprise technological security controls should be emailed by the CIO or EVP to ITS Leadership (itsleadership @fairfield.edu). The email should contain the length of time the disablement should occur. ITS Leadership will identity the appropriate resource to implement the disablement.
Routine requests that do not constitute disablement of enterprise technological security controls do not require special approval and should be submitted by the requestor to ITS through the ITS Help Desk.

For further assistance, please visit the ITS Help Desk located in NYS 230 or call 203-254-4069 during business hours.

Hours can be found here: ITS Help Desk Hours of Operation