

# Data Security Program

The State University of New York at Fredonia is committed to protecting the privacy of its students, alumni, faculty and staff, as well as protecting the confidentiality, integrity, and availability of information important to the University's mission. This program is used to determine the minimum security standards associated with our computing environment (e.g. data in transit and data at rest) in accordance with the [Data Risk Classification Policy](#).

## University Approved Software List

This table is for general data users across campus and indicates which risk classifications of data are permitted to be used with each University Approved Electronic Service.

### Fredonia Minimum Security Standards: Endpoints

An endpoint is defined as any laptop, desktop, or mobile device used to access the University computing infrastructure or data. Follow the minimum security standards in this table to safeguard your endpoints. NOTE: All personally owned endpoints that are use to access (store or transmit) University data are required to adhere to these Minimum Security Standards.

### Fredonia Minimum Security Standards: Servers

A server is defined as a computing host that provides a network accessible service. Follow the minimum security standards in this table to safeguard your servers.

### Fredonia Minimum Security Standards: Applications

An application is defined as software running on a server that is remotely accessible, including mobile applications. Follow the minimum security standards in this table to safeguard your applications.

### Fredonia ITS Support and Minimum Security Matrix

This table provides a general reference for minimum ITS support and security standards for the diverse computing environment across the University.

Please contact the Information Security Office at 673-4725 or [Information.Security@fredonia.edu](mailto:Information.Security@fredonia.edu) for if you need any assistance.