FLORIDA	**OFFICIAL**
POLYTECHNIC	**UNIVERSITY**
UNIVERSITY	**POLICY**

Subject/Title: Use of IT Resources when Remote
FPU Policy Number: FPU-11.0014P
_New Policy X Major Revision of Policy _Minor Technical Revision of Policy
Date First Adopted: September 23, 2015
Date Revised: April 9, 2020
Responsible Division/Department: Information Technology Services
Initiating Authority: Mark Mroczkowski, CFO

A. APPLICABILITY/ACCOUNTABILITY: This policy applies to all Florida Polytechnic University ("University") employees who use or access University IT Resources (the University network, technology and telecommunication resources, computing devices, or software including but not limited to computers, laptops, smartphones or other computing devices) while remote, away from University facilities and networks.

B. POLICY STATEMENT: The purpose of this policy is to minimize risk to University information technology and data incurred as a result of employees working while away from University facilities and networks. University employees are expected to exercise due diligence when using University IT Resources while remote from University facilities. Employees must comply with University policies to keep University data and IT resources secure. Remote work places devices at increased risk of loss or theft and the data on the device may be at risk from networks managed by entities that monitor and capture network traffic for competitive or malicious purposes.

C. POLICY:

1. Accessing the Internet:
    a. Employees using University-owned or employee-owned equipment must employ secure connections for computing and connecting to the University IT Resources and network, such as Hypertext Transport Protocol Secure (HTTPS) and/or a Virtual Private Network (VPN) so the connection does not compromise the security of the systems being used. Technology Services standards supporting this policy document appropriate encryption standards and tools.

b. Employees must not connect to University IT Resources from workstations not owned by the University or by the employee themselves, including public workstations or kiosks. Such workstations often capture login credentials and other highly restricted data from workstation users.

2. Protecting devices from theft: Mobile devices and equipment carrying any University data and information must not be left unattended and, where practical, must be physically secured.
3. Protecting data from theft:
    a. Mobile devices and equipment must be encrypted by industry standard whole disk encryption method. Employees must configure encryption on mobile devices they own; most mobile devices are configured appropriately by default. Technology Services standards supporting this policy document appropriate whole disk encryption methods.
    b. Mobile devices and equipment must be configured to unlock only with a secure password, PIN, or biometric authentication. Employees must configure secure unlock methods on mobile devices they own. Technology Services standards supporting this policy document password complexity requirements.
    c. Mobile devices and equipment must be configured with inactivity timeouts of a reasonably short duration of fifteen (15) minutes or less. Employees must configure inactivity timeouts on mobile devices they own.
    d. Data on mobile devices should be securely and remotely backed up as often as practical. Employees are encouraged to configure this capability on mobile devices they own.
    e. Operating system, security, anti-malware, and application patches must be installed on mobile devices as soon as practical. Where installation depends on employee action, employees must complete such action promptly.
4. Recovering lost or stolen devices: Remote wipe, tracing and tracking software must be used if practical. Employees are encouraged to configure this capability on mobile devices they own.
5. Notification of loss: In the event of theft or data compromise, employees must notify the University as soon as possible by contacting the Helpdesk by calling (863) 874-8888 or emailing helpdesk@floridapoly.edu.
6. Remote access to University email and data files. As the terms are defined in FPU-11.00122P - Data Classification and Protection, employees must not store highly restricted or restricted University data on personal cloud storage services. Instead, employees can access data using a University-sanctioned cloud storage service: currently University-provisioned Microsoft OneDrive or SharePoint. Employees are responsible for retaining all University data in

compliance with applicable record retention schedules regardless of where the data is stored.

7. Consequences of violating policy. Employees who violate this policy may be subject to disciplinary action up to and including termination.

To the extent that this policy governs automated business processes, these procedures are documented within the University's Enterprise Resource Planning (ERP) system. Any/all other procedures governed by this policy, will reside on Technology Services Department's website.

POLICY APPROVAL

Policy No.:11.0014P

_____	_____
Initiating Authority	Date
_____	_____
Policies & Procedures Review Committee Chair	Date
_____	_____
President/Designee	Date
Approved by FPU BOT, if required	_____
	Date

EXECUTED SIGNATURE PAGES ARE AVAILABLE IN THE OFFICE OF THE GENERAL COUNSEL