TigerFlex Pilot Program Technology Deployment Process

I. Pilot Program Principles for Technology Deployment

This process addresses how Auburn University will deploy remote access technologies to securely and effectively facilitate various options for working remotely during the pilot project.

This process applies to all of the following to include endpoints, publicly accessible computing environments (such as “hoteling spaces”), public Internet services and personal subscriptions to commercial Internet-based services that enable access to Auburn’s technical infrastructure form a remote location.

Remote access is governed by the same Auburn policies as on-campus use of technical infrastructure augmented by the additional requirements stated in this process.

During the pilot phase only Auburn-provided computers and tablets are to be used for computational purposes. Personally-owned smartphones, computer monitors, and printers may be used.

II. Technical Eligibility

Participants and their unit head must be able to meet the following technical requirements:

- Ability to comply with all requirements in this Technology Deployment Process.
- Agreement by the department head to commit the department technology team to maintaining all systems used remotely.

III. Pilot Program Operating Environment

For the duration of the Remote Work Pilot Project, remote access will be provide to faculty and staff to assess how effectively they can complete their official duties when working in various off-campus locations. However, the Chief Information Officer (CIO), the Deputy Chief Information Officer (DCIO) or Chief Information Security Officer (CISO) may withdraw remote access at any time, without prior notice, when necessary to protect information security or systems or for other administrative reasons. The CIO, DCIO, and/or CISO may consult with other administrators as needed in evaluating remote access revocations.

IV. Deployment of Technology

A. Employees who are approved for remote access will use one of the following three computing equipment deployment options based upon the format of remote work.

For Those Working Remotely 2-3 Days Per Week

- A campus provided laptop: Auburn will not provide a monitor at the remote location. However, any Auburn-owned monitor scheduled for surplus may be redeployed to the remote work location.
- A personal monitor may be used if available.

For Those Working Remotely 100% of Their Workday

- Any Auburn-owned computing device may be used regardless of form factors (desktop, laptop, tablet)
- Any Auburn-owned monitor scheduled for surplus may be redeployed to the remote work location.

For Those Working Remotely but Periodically Utilizing a "Hoteling Space"

- A campus provided laptop with an Auburn-owned monitor scheduled for surplus or a personal monitor will be used at the remote work location.
- The hoteling space will offer only a network connection. That connection will be a Wifi connection to the EDUROAM network. Monitors may/may not be available at the hotel space.

B. All computing devices used for remote access will use the following cybersecurity suite of tools to prevent malware from infecting the machine or the campus network

- DUO 2Factor Security
- Global Protect Virtual Private Network
- AMP Antivirus/Firewall
- Umbrella for Desktop

C. Printing in a remote location is discouraged. Auburn will not provide a printer or printer supplies. If a personal printer is used, the staff or faculty member working remotely must have access to a cross-cut shredder and shred all documents when no longer needed. If documents are to be saved at the remote work location they must be saved in a secure space.

D. Any security breach, or suspected security breach, will be reported immediately to the department IT professional who will notify the CIO, DCIO or Chief Information Security Officer.

E. Employees will not be reimbursed for personal cellular service, Internet service, equipment, supplies, accessories or furniture.

F. All faculty and staff working remotely will maintain a log of significant technical events that may help improve remote access services. Log entries may be events that caused difficulties and/or problems. Those log entries may also note tools, techniques, and processes found to be particularly effective.

V. Definitions

- **CFO – Chief Financial Officer**: The campus executive responsible for all financial transactions, operations, and strategic budget and forecasting programs.

- **CIO - Chief Information Officer**: The campus executive responsible for all information technology policy, strategy and central technology services at Auburn University.

- **DCIO – Deputy Chief Information Officer**: The campus official charged with day-to-day management of all central information technology services. Functions as the senior leader for campus information technology in the absence of the CIO.

- **CISO – Chief Information Security Officer**: The campus official charged with assuring all information technology assets are secure across the entire enterprise. Responsible for recommending and assessing cybersecurity policy.

VI. Sanctions

Violations of this procedure may result in the faculty or staff member being held personally responsible for all costs resulting from remediating the violation.

Deliberate disregard of the requirements stated in this procedure may result in the faculty or staff member being removed from the pilot project. Disregard of cybersecurity standards may result in disciplinary action up to and including dismissal.

VII. Officials Responsible for Project Management

- **Executive Responsible for Remote Work Pilot**: Office of the VP for Finance/CFO
- **Executive Responsible for Technology Deployment**: Office of the VPIT/CIO
- **Officer Responsible for Cybersecurity**: Chief Information Security Officer