The purpose of this document is to walk non-IT professionals through the FY19 Non-IT Professional IT Risk Assessment designed for assessing end-user devices.

FY19 Texas A&M Non-IT Professional IT Risk Assessment - Sole Custodian: End-User Device

All information resources (workstations, laptops, tablets, servers, etc.) are required to be assessed per Texas Administrative Code 202 (TAC 202) and TAMU Rule 29.01.03.M0.01 Procedure 3.

This IT risk assessment must be completed by individuals who are the sole custodians for managing one or more desktops, laptops, and/or tablets.

Depending on configurations, all information resources may be included in one IT risk assessment.

The questions asked in this assessment are related to the Texas A&M University (TAMU) security control catalog.

The IT risk assessment is divided into sections. Each section focuses on a specific area of managing information resources.

All questions in each section are required to be answered. Your selected answers for some questions will determine the next section that needs to be filled out. This is done to reduce answering questions that do not apply to how the information resource(s) is managed.

The responses will be sent to the email address you provide.

Section 1: General Information	
Section comment(s):	This section is used to gather information about the information resource(s). Assistance for question a: All information resources on the Texas A&M network have a name. • For Windows operating systems (OS): Control Panel -> System and Security -> System -> look for "Full computer name:" under the "Computer name, domain, and workgroup settings" section. • For Apple OS: Apple menu -> System Preferences -> then click Sharing -> then look for "Computer Name" Assistance for question b: TAMU asset number used for/listed in FAMIS/Canopy, department level identification numbers, etc. Most departments add a service tag label on information resources before distributing to employees that help track it for general inventory management practices. This tag is often easily visible on the information resource.
a	**Name(s) for the information resource(s):**
Comment(s)	Separate multiple names with a comma.

b	**Information resource(s) identification number(s) used by the unit:**
Comment(s)	Separate multiple identification numbers with a comma.
c	**Quantity:**
Comment(s)	Provide the number of information resources included in this assessment. Enter that number (e.g. 1, 2, 3)
d	**Information resource(s) description:**
Comment(s)	Briefly, tell us a about this information resource(s) and what it is used for. For example: "This workstation is my primary office workstation used for administrative and academic tasks." or "This includes my office workstation, the research cluster, a lab of computers, and my tablet. These resources are used to support my teaching and research."
e	**Hardware type(s):**
Comment(s)	Select each option that applies to the information resource(s).
Answer Choices:	Desktop, Laptop , Tablet or other mobile device
f	**Operating system (OS):**
Comment(s)	Select all applicable operating systems for the information resource(s).
Answer Choices:	Windows, macOS, Linux or other UNIX, Android OS (mobile), iOS (Apple mobile), Chrome OS, Other
g	**Number of people with authorized access to the information resource(s):**
Comment(s)	Enter a number (e.g. 1, 2, 3)

Section 1a: Data Classification	
Section comment(s):	This section is used to gather information about the data classification and Social Security Number (SSN) scanning on the information resource(s).
h	**Is confidential data (e.g. SSNs, Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Personally Identifiable Information (PII), etc.) stored on the information resource(s)?**
Comment(s)	In general, accessing confidential data via applications (email, shared networked storage, web browser, etc.) does not mean you are storing confidential information on the information resource(s) itself. However, if you make a copy from one of these applications and save locally (e.g. drag-and-drop, save, copy-paste a file, save email, etc.), you are storing confidential data on the information resource(s).
Answer Choices:	Unknown, No, Yes
i	**Is the information resource(s) scanned for SSNs by using a software tool (e.g. Identity Finder) and/or is whole disk encryption used to protect data stored on the information resource(s)?**

Answer Choices:	Scan, Whole Disk Encryption, Both - Scan and Whole Disk Encryption, None of the above

Section 2: Access Management							
Section comment(s):	Section 2 is the start of the assessment and focuses on access, user accounts, passwords, authentication systems, etc. The question(s) in this section relate to requirements found in TAMU security control(s): Account Management (AC-2), Separation of Duties (AC-5), System Use Notification (AC-8), Session Lock (AC-11), Identification and Authentication (Organizational Users) (IA-2), Identifier Management (IA-4)						
1	**Is an access banner displayed during authentication?**						
Answer Choices:	No banner	Information resource lacks banner functionality	Displayed banner does not meet TAMU Security Control AC-8	Displayed banner meets TAMU Security Control AC-8			
2	**Is a complete and current procedure in place for granting access?**						
Answer Choices:	Procedure does not exist or is incomplete	Procedure reviewed >12 months ago	Procedure reviewed <12 months ago				
3	**Do formal procedures exist for changing shared account (root, administrator, etc.) passwords when staff or duties change?**						
Answer Choices:	No	Yes, but not documented	Yes, documented	No shared accounts exist			
4	**How long can an information resource be left unattended before the screen is locked?**						
Answer Choices:	No screen lock	Screen lock >30 minutes	Screen lock between 15-30 minutes	Screen lock <15 minutes			
5	**Does the information resource use university central authentication (NetID)?**						
Answer Choices:			No	Yes, but alternate authentication sources are available	Yes, exclusively university central authentication		

Next Section:	**Depends on answer choice for question 5.**	**Section 2a: Access Management (pg 4)**	**Section 2a: Access Management (pg 4)**	**Section 3: Resource Maintenance (pg 7)**		

Answer these questions if: "No" or "Yes, but alternate authentication sources are available" was the answer for question 5 in Section 2.

Section 2a: Access Management							
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Account Management (AC-2), Separation of Duties (AC-5), Identification and Authentication (Organizational Users) (IA-2), Identifier Management (IA-4)						
6	**Are usernames/user IDs unique?**						
Answer Choices:	Users are not identified	Shared names/IDs are used	Shared & Unique names/IDs are used	Only Unique names/IDs are used			
7	**Do any non-university personnel (e.g. students who are not student workers, vendors, etc.) have an account or access to an account (e.g. borrowing account credentials, temporary account credentials) on the information resource(s)?**						
Answer Choices:	Unknown	No	Yes				
8	**How often are accounts (e.g. standard and elevated) reviewed for deactivation (due to inactivity, termination, etc.)?**						
Answer Choices:	Accounts are not reviewed	Ad hoc reviews & updates	Within 72 hours	Within 24 hours	Realtime based on event triggers		
9	**Are deactivated/disabled accounts removed after a set time period?**						
Answer Choices:	No	> 6 months	Within 6 months				
10	**Does the authentication method utilize passwords?**						

Answer Choices:			Passwords are not used	Passwords are used	N/A - use other form of authentication		
Next Section:	**Depends on answer choice for question 10.**		**Section 2d: No Authentication (pg 6)**	**Section 2b: Password Management (pg 5)**	**Section 2c: Authentication (pg 6)**		

Answer these questions if: "Passwords are used" was the answer for question 10 in Section 2a.

Section 2b: Password Management							
Section comment(s):	The question(s) in this section relate to password requirements found in TAMU security control(s): Authenticator Management (IA-5)						
11	**What is the minimum password length available to users?**						
Answer Choices:	Allows blank passwords	Allows < 8 characters passwords	Requires at least 8 characters	Requires > 15 character passwords			
12	**What are the minimum password complexity requirements being enforced?**						
Comment(s):	If the password is at least 16 characters long, then users are not required to meet the complexity requirements.						
Answer Choices:	No complexity requirements	Requires 1 or 2 of the following 4 groups of characters: lower case letters, upper case letters, symbols or numbers	Requires 3 of the following 4 groups of characters: lower case letters, upper case letters, symbols or numbers	Requires 4 of the following 4 groups of characters: lower case letters, upper case letters, symbols or numbers	At least 16 characters required - no complexity requirement		
13	**How often are users forced to change their passwords?**						
Answer Choices:	Password changes are not forced	Greater than a year	Requires annual changes	Requires semi-annual changes	Requires quarterly changes	At least 16 characters required - never expires	

14	**How many consecutive invalid access attempts are allowed before automatically locking the account or delaying the next login prompt?**						
Answer Choices:	No account locking	>10 attempts	10 or less attempts				
15	**How long before the system re-enables an account after an account lockout?**						
Answer Choices:	Immediately	<15 minutes	15 minutes or longer	Locked until administrator reset			
Next Section:	**Section 3: Resource Maintenance (pg 7)**						

Answer these questions if: "N/A - use other form of authentication" was the answer for question 10 in Section 2a.

Section 2c: Authentication	
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Identification and Authentication (Organizational Users) (IA-2)
11	**What form of authentication is used?**
Answer Choices:	free text
12	**How do you ensure that users are not sharing accounts/credentials??**
Answer Choices:	free text
Next Section:	**Section 3: Resource Maintenance (pg 7)**

Answer these questions if: "Passwords are not used" was the answer for question 10 in Section 2a.

Section 2d: No Authentication	
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Permitted Actions without Identification or Authentication (AC-14)
11	**What activities can be performed on the information resource(s) without identification or authentication?**
Answer Choices:	free text
12	**Why is authentication not used before accessing the information resources?**

Answer Choices:	free text
Next Section:	**Section 3: Resource Maintenance (pg 7)**

Section 3: Resource Maintenance							
Section comment(s):	Section 3 focuses on how the information resource(s) is maintained. The question(s) in this section relate to requirements found in TAMU security control(s): Separation of Duties (AC-5), Configuration Management Policy and Procedures (CM-1), User Installed Software (CM-11), Security Categorization (RA-2), Malicious Code Protection (SI-3)						
1	**Is the installed version of the operating system (OS) officially supported by the vendor?**						
Answer Choices:	No	No, but an exception request has been completed and approved	Yes				
2	**Is only appropriately licensed software installed on the information resource(s)?**						
Comment(s):	Freeware versions of non-open source software are likely to contain malware.						
Answer Choices:	Unknown	No	Yes				
3	**Are any unsupported applications installed (no longer receiving application or security updates from the vendor)?**						
Answer Choices:	Unknown	Yes	No, but with exceptions	No			
4	**Is a documented process followed for updating the information resource(s)?**						
Answer Choices:	No	Yes					
5	**How long until the information resource(s) is updated after the vendor releases an OS security update?**						
Answer Choices:	Do not update	Ad hoc updating	Updated < 90 days	Updated < 60 days	Updated < 30 days		
6	**Is the transfer of information to/from removable media monitored by data loss protection (DLP) software?**						
Answer Choices:	No	No, but with exceptions	Yes	Yes - use the university supplied software			

7	Is the university-supplied anti-virus/anti-malware installed?						
Answer Choices:			No	No, but an exception request has been completed and approved	Yes		
Next Section:	**Depends on answer choice for question 7.**		**Section 3a: Anti-virus/Anti-malware (pg 8)**	**Section 3a: Anti-virus/Anti-malware (pg 8)**	**Section 4: Backups (pg 8)**		

Answer this question if: "No" or "No, but an exception request has been completed and approved" was the answer for question 7 in Section 3.

Section 3a: Anti-virus/Anti-malware							
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Malicious Code Protection (SI-3)						
8	**Are current anti-virus/anti-malware software and definitions installed?**						
Answer Choices:	No virus control	Outdated virus control	Manual updated virus control	Auto-updated virus control			
Next Section:	**Section 4: Backups (pg 8)**						

Section 4: Backups							
Section comment(s):	Section 4 focuses on backups for the information resource(s). The question(s) in this section relate to requirements found in TAMU security control(s): Information System Backup (CP-9)						
1	**Are data backups performed?**						
Answer Choices:			No	Yes	Yes - 3rd party/vendor responsibility		
Next Section:	**Depends on answer choice for question 1.**		**Section 5: Logs (pg 9)**	**Section 4a: Backups (pg 9)**	**Section 4a: Backups (pg 9)**		

Answer these questions if: "Yes" was the answer for question 1 in Section 4.

Section 4a: Backups							
Answer Choices:	The question(s) in this section relate to requirements found in TAMU security control(s): Information System Backup (CP-9)						
2	**How often are data backups performed?**						
Answer Choices:	Ad hoc backups	Monthly backups	Weekly backups	Daily backups			
3	**Are the backup media encrypted?**						
Answer Choices:	No	Yes, but with exceptions	Yes	N/A - no restricted or confidential data			
Next Section:	**Section 5: Logs (pg 9)**						

Section 5: Logs							
Section comment(s):	Section 5 focuses on logs for the information resource(s). The question(s) in this section relate to requirements found in TAMU security control(s): Audit Events (AU-2), Audit Generation (AU-12)						
1	**Where are logs stored?**						
Comment(s):	A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.						
Answer Choices:			Unknown or no logs are stored	Logs stored locally	Logs sent to external server	Logs sent to Division of IT Splunk service	
Next Section:	**Depends on answer choice for question 1.**		**Done**	**Section 5a: Logs (pg 9)**	**Section 5a: Logs (pg 9)**	**Section 5b: Logs (pg 10)**	

Answer these questions if: "Logs stored locally" or "Logs sent to external server" was the answer for question 1 in Section 5.

Section 5a: Logs

Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Audit Events (AU-2), Content of Audit Records (AU-3), Protection of Audit Information (AU-9), Audit Generation (AU-12), Information System Monitoring (SI-4)						
2	**Are the date and time recorded with each logged event?**						
Answer Choices:	Date & Time are not recorded	Date & Time are recorded					
3	**Do logged events include the User IDs?**						
Answer Choices:	No	Yes					
4	**Are authentication attempts logged?**						
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts				
5	**Are controls in place to prevent the deletion or modification of logs?**						
Answer Choices:	Logs are not protected	Logs are protected					
Next Section:	**Done**						

Answer these questions if: "Logs sent to Division of IT Splunk service" was the answer for question 1 in Section 5.

Section 5b: Logs							
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Audit Events (AU-2), Content of Audit Records (AU-3), Information System Monitoring (SI-4)						
2	**Do logged events include the User IDs?**						
Answer Choices:	No	Yes					
3	**Are authentication attempts logged?**						
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts				

Next Section:	**Done**