The purpose of this document is to walk non-IT professionals with elevated privileges through the FY19 Non-IT Professional IT Risk Assessment - Elevated Privileges assessment.

FY19 Texas A&M Non-IT Professional IT Risk Assessment - Elevated Privileges

All information resources (workstations, laptops, tablets, servers, etc.) are required to be assessed annually, 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 have elevated privileges on one or more information resources. 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.

Section 1 is used to gather information about what is being assessed. The assessment starts in Section 2.

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):	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	**Hardware type(s):**
Comment(s):	Select each option that applies to the information resource(s).
Answer Choices:	Desktop; Laptop; Tablet or other mobile device
e	**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
f	**Where is the information resource(s) used?**
Comment(s):	Select each option that applies to the information resource(s).
Answer Choices:	At the university when unit IT support is available; At the university when unit IT support is not available (e.g. weekends and nights); At home; While traveling; Other

Section 1a: Data Classification	
Section comment(s):	This section focuses on data classification of the information resource(s).
g	**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

Section 2: Access Management	
Section comment(s):	This section is the start of the assessment and focuses on user account access, passwords, authentication systems, etc. The question(s) in this section relate to requirements found in TAMU security control(s): Account Management (AC-2), Identifier Management (IA-4)
1	**Do you create or manage any user accounts for the information resource(s)?**

Answer Choices:			Yes	No			
2	**Are the authentication credentials (user ID and password) for your elevated privilege account different than the authentication credentials for your standard user account?**						
Answer Choices:	No	Yes					
3	**Is your unit IT staff responsible for the management of authentication requirements (e.g. user accounts, passwords) for the information resource(s)?**						
Answer Choices:			No	Yes but I also create or manage accounts	Yes		
Next Section:	**Depends on answer choice for question 3.**		**Section 2a: Access Management (Pg 3)**	**Section 2a: Access Management (Pg 3)**	**Section 3: Resource Maintenance (Pg 6)**		

Answer these questions if "No" or "Yes but I also create or manage accounts"was the answer for question 3 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)						
4	**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			
5	**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			

6	**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		
7	**Are deactivated/disabled accounts removed after a set time period?**						
Answer Choices:	No	> 6 months	Within 6 months				
8	**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 8.**		**Section 2d: No Authentication (Pg 6)**	**Section 2b: Password Management (Pg 4)**	**Section 2c: Authentication (Pg 5)**		

Answer these questions if "Passwords are used" was the answer for question 8 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)						
9	**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			
10	**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		
11	**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	
12	**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				
13	**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 6)**						

Answer these questions if "N/A - use other form of authentication" was the answer for question 8 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)
9	**What form of authentication is used?**
Answer Choices:	free text
10	**How do you ensure that users are not sharing accounts/credentials??**

Answer Choices:	free text
Next Section:	**Section 3: Resource Maintenance (Pg 6)**

Answer these questions if "Passwords are not used" was the answer for question 8 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)
9	**What activities can be performed on the information resource(s) without identification or authentication?**
Answer Choices:	free text
10	**Why is authentication not used before accessing the information resources?**
Answer Choices:	free text
Next Section:	**Section 3: Resource Maintenance (Pg 6)**

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	**Do you use your elevated privileges solely on information resources that are assigned to you?**						
Answer Choices:	No	Yes	N/A - elevated account is only activated for the assigned information resources				
2	**Do you use the elevated privileges only when needed (to install software or updates) and not used in place of your standard user account?**						

Answer Choices:	No - only have one account, my standard user account also grants elevated privileges	No - I have a separate admin account but I use it most of the time	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	**If you have installed software on the information resource(s), do you update the software within 90 days when the vendor releases a security update?**						
Answer Choices:	No	Yes, but with exceptions	Yes	N/A - do not manage any software			
5	**Is all software installed on the information resource(s) appropriately licensed software?**						
Answer Choices:	No	Yes, but with exceptions	Yes				
6	**Do you override any unit IT workstation policy settings on the information resource(s)?**						
Answer Choices:	Yes	No					
7	**Is your unit IT staff responsible for the management of the operating system (OS) and anti-virus on the information resource(s)?**						
Answer Choices:			No	Unit IT staff is responsible for anti-virus only	Unit IT staff is responsible for OS only	Yes	
Next Section:	**Depends on answer choice for question 7.**		**Section 3a: Anti-virus/Anti-malware and Operating System (Pg 9)**	**Section 3c: Operating System and Logs (Pg 8)**	**Section 3b: Anti-virus/Anti-malware (Pg 8)**	**Done**	

Answer this question if "Unit IT staff is responsible for OS only" was the answer for question 7 in Section 3.

Section 3b: 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	**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 8.**		**Section 3d: Anti-virus/Anti-malware (Pg 8)**	**Section 3d: Anti-virus/Anti-malware (Pg 8)**	**Done**		

Answer this question if "No" or "No, but an exception request has been completed and approved" was the answer for question 8 in Section 3b.

Section 3d: 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)						
9	**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:	**Done**						

Answer this question if "Unit IT staff is responsible for anti-virus only" was the answer for question 7 in Section 3.

Section 3c: Operating System and Logs

Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Configuration Management Policy and Procedures (CM-1), Security Categorization (RA-2), Malicious Code Protection (SI-3), Audit Events (AU-2), Audit Generation (AU-12)						
8	**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				
9	**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		
10	**Is the information resource(s) scanned for SSNs by using a software tool (e.g. Identity Finder) and/or is whole disk encryption used**						
Answer Choices:	Scan	Whole Disk Encryption	Both - Scan and Whole Disk	Responsibility of unit IT staff	None of the above		
11	**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 11.**		**Done**	**Section 3h: Logs (Pg 12)**	**Section 3h: Logs (Pg 12)**	**Section 3g: Logs (pg 11)**	

Answer this question if "No" was the answer for question 7 in Section 3.

Section 3a: Anti-virus/Anti-malware and Operating System	
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Configuration Management Policy and Procedures (CM-1), Security Categorization (RA-2), Malicious Code Protection (SI-3)
8	**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				
9	**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		
10	**Is the information resource(s) scanned for SSNs by using a software tool (e.g. Identity Finder) and/or is whole disk encryption used**						
Answer Choices:	Scan	Whole Disk Encryption	Both - Scan and Whole Disk	Responsibility of unit IT staff	None of the above		
11	**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			
12	**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 12.**		**Section 3e: Anti-virus/Anti-malware and Logs (pg 10)**	**Section 3e: Anti-virus/Anti-malware and Logs (pg 10)**	**Section 3f: Logs (pg 11)**		

Answer this question if "No" or "No, but an exception request has been completed and approved" was the answer for question 12 in Section 3a.

Section 3e: Anti-virus/Anti-malware and Logs	
Section comment(s):	The question(s) in this section relate to requirements found in TAMU security control(s): Malicious Code Protection (SI-3), Audit Events (AU-2), Audit Generation (AU-12)
13	**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			
14	**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 14.**		**Done**	**Section 3h: Logs (Pg 12)**	**Section 3h: Logs (Pg 12)**	**Section 3g: Logs (pg 11)**	

Answer these questions if "Yes" was the answer for question 12 in Section 3a.

Section 3f: 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)						
13	**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 13.**		**Done**	**Section 3h: Logs (Pg 12)**	**Section 3h: Logs (Pg 12)**	**Section 3g: Logs (pg 11)**	

Answer these questions if "Logs sent to Division of IT Splunk service" was the answer for question 11 in Section 3c, question 14 in Section 3e, or question 13 in Section 3f.

Section 3g: 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)						
	Do logged events include the User IDs?						
Answer Choices:	No	Yes					
	Are authentication attempts logged?						
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts				
Next Section:	**Done**						

Answer these questions if "Logs stored locally" or "Logs sent to external server" was the answer for question 11 in Section 3c, question 14 in Section 3e, or question 13 in Section 3f.

Section 3h: 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)						
	Are the date and time recorded with each logged event?						
Answer Choices:	Date & Time are not recorded	Date & Time are recorded					
	Do logged events include the User IDs?						
Answer Choices:	No	Yes					
	Are authentication attempts logged?						
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts				
	Are controls in place to prevent the deletion or modification of logs?						
Answer Choices:	Logs are not protected	Logs are protected					

Next Section:	**Done**