The purpose of this document is to walk individuals with elevated privileges through the *2020 IT Risk Assessment - Elevated Privileges* assessment.

2020 IT Risk Assessment - Elevated Privileges

At Texas A&M, state law requires us to perform annual risk assessments for all IT resources (laptops, servers, applications, etc.). Usually this assessment is performed by professional IT staff for your unit, but in some cases it must be completed by individuals who manage or have admin rights on an IT resource.

The questions asked in this assessment are directly related to a security requirement which must be followed by anyone that manages an IT resource. When possible, we've provided a link directly to the university requirement that prompted each question.

This assessment has four main sections. Section 1 is used to gather general information; the assessment questions start in Section 2. Your answers for some questions will determine the questions in the next section; this is done to skip questions that do not apply to your IT resource.

A copy of the assessment results will be sent to the email address provided below.

Section 1: General Information	
Section comments:	Section 1 is for gathering general information about the IT resource being assessed.
a	**Name for the IT resource:**
Comments:	Separate multiple names with a comma. IT resources on the Texas A&M network have a name. For Windows: Control Panel ⟶ System and Security ⟶ System ⟶ look for "Full computer name:" under the "Computer name, domain, and workgroup settings" section. For macOS: Apple menu ⟶ System Preferences ⟶ then click Sharing ⟶ then look for "Computer Name"
b	**IT resource identification number used by the unit:**
Comments:	Separate multiple identification numbers with a comma. TAMU asset number used for/listed in FAMIS/Canopy, department level identification numbers, etc. Most departments add a service tag label on IT resources before distributing to employees that help track it for general inventory management practices. This tag is often easily visible on the IT resource.
c	**Quantity:**
Comments:	Provide the number of IT resources included in this assessment. Enter that number (e.g. 1, 2, 3)
d	**Hardware type:**

Comments:	Select the option that best applies to the IT resource.						
Answer Choices:	Desktop / Laptop	Tablet or other mobile device	Server	Other			
e	**Operating system (OS):**						
Comments:	Select the applicable operating system for the IT resource.						
Answer Choices:	Windows	macOS	Linux or other UNIX	Chrome OS	Other		
f	**What is the highest category of data stored or processed by this IT resource?**						
Comments:	If you are not sure how to classify the data, use the data classification calculator in the link below.						
Data calculator:	https://u.tamu.edu/datacalc						
Answer Choices:	Public	University-Internal	Confidential	Critical			

Section 2: Access Management							
Section comments:	Section 2 is the start of the assessment and focuses on user account access, passwords, authentication systems, etc. It is broken up into parts based on the answers provided.						
1	**Do you create or manage any user accounts for the IT resource?**						
Answer Choices:	No	Yes					
2	**Is your unit IT staff responsible for the management of authentication requirements (e.g., user accounts, passwords) for the IT resource?**						
Answer Choices:			No	Yes but I also create or manage accounts	Yes		
Next Section:	**Depends on answer choice for question 2.**		**2a: Access Management (Pg 2)**		**Section 3: Resource Maintenance (Pg 6)**		

Only answer these questions if "No" or "Yes but I also create or manage accounts"was the answer for question 2 in Section 2.

2a: Access Management	
Section comments:	This part of Section 2 focuses on user account access, authentication systems, etc.

1	**Is a documented procedure in place for granting access?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	No documented procedure exists		Yes, a documented procedure exists				
2	**Are User IDs (usernames) unique?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	Shared IDs are used	Shared & unique IDs are used	Only unique IDs are used				
3	**Do any third parties (e.g., research affiliates, business associates, service providers, vendors, contractors) have access to the IT resource?**						
Answer Choices:	No	Yes					
4	**Is a documented process in place for the granting and removal of access to third parties?**						
Requirement:	https://it.tamu.edu/cc/IA-8						
Answer Choices:	No documented process exists		Yes, a documented process exists		N/A - no third party will ever be granted access		
5	**Is an access banner displayed during authentication?**						
Requirement:	https://it.tamu.edu/cc/AC-8						
Comments:	Per AC-8, the login notification (access banner) shall address the following items: (1) Unauthorized use is prohibited; (2) Usage may be subject to security testing and monitoring; (3) Misuse may be subject to criminal prosecution; (4) Users have no expectation of privacy except as otherwise provided by applicable privacy laws; and (5) A reference to University Standard Administrative Procedure 29.01.03.M0.02, Rules for Responsible Computing.						
Answer Choices:	No banner	IT resource lacks banner functionality	Displayed banner does not meet TAMU Security Control AC-8	Displayed banner meets TAMU Security Control AC-8			
6	**How long can an IT resource be left unattended before the screen is locked?**						
Requirement:	https://it.tamu.edu/cc/AC-11						
Answer Choices:	No Screen lock	Screen lock after 30 minutes	Screen lock after 15 minutes	Screen lock at or before 15 minutes			

7	**How often are accounts (e.g., standard and elevated) reviewed for deactivation (due to inactivity, termination, etc.)?**						
Requirement:	https://it.tamu.edu/cc/PS-4						
Answer Choices:	Accounts are not reviewed	Ad hoc reviews & updates	Within 72 hours	Within 24 hours	Realtime based on event triggers		
8	**Are deactivated/disabled accounts removed after a set time period?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	No	> 6 months	Within 6 months				
9	**What authentication method is utilized?**						
Requirement:	https://it.tamu.edu/cc/IA-2						
Answer Choices:			No authentication required	Pin code	Passwords	Biometrics	
Next Section:	**Depends on answer choice for question 9.**		**2c: No Authentication (Pg 6)**	**2b: Password Management (Pg 4)**		**Section 3: Resource Maintenance (Pg 6)**	

Only answer these questions if "Pin code" or "Passwords" was the answer for question 9 in 2a.

2b: Password Management						
Section comments:	This part of Section 2 focuses on password and/or pin code requirements.					
1	**What is the minimum required password length?**					
Requirement:	https://it.tamu.edu/cc/IA-2					
Answer Choices:	Allows blank passwords	Allows < 8 characters passwords	Requires at least 8 characters	Requires > 15 character passwords		
2	**What are the minimum password complexity requirements being enforced?**					
Requirement:	https://it.tamu.edu/cc/IA-2					
Comments:	If less than 16 characters, password must contain three of the following four groups of characters: lower case letters, upper case letters, symbols or numbers. If the password is at least 16 characters long, there are no complexity requirements.					

Answer Choices:	No complexity requirements	Some complexity requirements	Requires 3 of the following 4 groups of characters: lower case letters, upper case letters, symbols or numbers		At least 16 characters required - no complexity requirement		
3	**Is the password complexity enforced when a password is created or changed by a user?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
Comments:	If the password is at least 16 characters long, then users are not required to meet the complexity requirements.						
Answer Choices:	No	Yes					
4	**How often are users forced to change their passwords?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
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	
5	**When authentication fails, is the user informed of which portion of the authentication process failed?**						
Requirement:	https://it.tamu.edu/cc/IA-6						
Answer Choices:	Message indicates if it was the User ID (username) or password that failed		Message provides no indication as to the failure reason				
6	**How many consecutive invalid access attempts are allowed before automatically locking the account or delaying the next login prompt?**						
Requirement:	https://it.tamu.edu/cc/AC-7						
Comments:	Account lockouts help against brute force attacks.						
Answer Choices:	No account locking	>10 attempts	10 or less attempts				
7	**How long before the system re-enables an account after an account lockout?**						
Requirement:	https://it.tamu.edu/cc/AC-7						
Answer Choices:	No account locking	Immediately	<15 minutes	15 minutes or longer	Locked until administrator reset		
Next Section:	**Section 3: Resource Maintenance (Pg 6)**						

Only answer these questions if "No authentication required" was the answer for question 9 in 2a.

2c: No Authentication	
Section comments:	This part of Section 2 follows up on why authentication is not used.
1	**What activities can be performed on the IT resource without identification or authentication?**
Requirement:	https://it.tamu.edu/cc/AC-14
Answer Choices:	free text
2	**Why is authentication not used before accessing the IT resource?**
Requirement:	https://it.tamu.edu/cc/AC-14
Answer Choices:	free text
Next Section:	**Section 3: Resource Maintenance (Pg 6)**

These questions must always be answered.

Section 3: Resource Maintenance					
Section comments:	Section 3 focuses on how the IT resource is maintained. It is broken up into parts based on the answers provided.				
1	**Do you use your elevated privileges solely on IT resources that are assigned to you?**				
Requirement:	https://it.tamu.edu/cc/AC-5				
Comments:	This includes sharing your account information with other people.				
Answer Choices:	No, I use my elevated privileges on multiple IT resources	Yes, the elevated account is only used on assigned IT resources			
2	**Do you use the elevated privileges only when needed (to install software or updates)?**				
Requirement:	https://it.tamu.edu/cc/AC-6				
Comments:	Examples of day-to-day tasks: checking email, web browsing, etc.				

Answer Choices:	I use the elevated privilege account most of the time, including day-to-day tasks		Elevated privileges are only used when needed: day-to-day tasks are not performed with elevated privileges				
3	**Do you manage any applications or software on the IT resource?**						
Comments:	Managing software or applications may include updating it, ensuring the it is appropriately licensed, etc.						
Answer Choices:			No	Yes			
Next Section:	**Depends on answer choice for question 3.**		**3b: Security Management (Pg 8)**	**3a: Application Management (Pg 7)**			

Only answer these questions if "Yes" was the answer for question 3 in Section 3.

3a: Application Management							
Section comments:	This part of Section 3 follows up on managing applications or software within the IT resource.						
1	**Are any unsupported applications and/or software installed (e.g., the application is no longer receiving security updates from the vendor or development organization)?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Answer Choices:	No	Yes, but an exception has been approved by the CISO		Yes			
2	**How long after a security update is released before the application and/or software is updated?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Comments:	Security updates for the application and/or software are released by vendor or development organization.						
Answer Choices:	greater than 60 days	within 60 days	within 30 days	Immediately			
3	**Is the application and/or software installed appropriately licensed?**						
Requirement:	https://it.tamu.edu/cc/CM-11						
Comments:	Free versions of proprietary software are likely to contain malware.						
Answer Choices:	No	Yes					

Next Section:	**3b: Security Management (Pg 8)**					

These questions must always be answered.

3b: Security Management							
Section comments:	This part of Section 3 focuses on security management of the IT resource.						
1	**Do you override any security settings put in place by your IT staff?**						
Requirement:	https://it.tamu.edu/cc/CM-6						
Answer Choices:	No	Yes					
2	**Do you make changes to any security tools (e.g., anti-virus software, firewall, etc.) installed by your IT staff?**						
Requirement:	https://it.tamu.edu/cc/CM-6						
Comments:	Changes can include disabling, bypassing, or altering.						
Answer Choices:	No	Yes	N/A - unit IT staff did not install any security tools				
3	**Is your unit IT staff responsible for managing the operating system (OS) (including university required security tools like antivirus & data loss protection)?**						
Answer Choices:			No	Yes			
Next Section:	**Depends on answer choice for question 3.**		**3c: Resource Maintenance (Pg 8)**	**Done**			

Only answer these questions if "No" was the answer for question 3 in 3b.

3c: Resource Maintenance	
Section comments:	This part of Section 3 focuses on resource management when the unit IT staff does not manage the OS.

1	**Is the installed version of the operating system (OS) officially supported by the vendor?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Answer Choices:	No	No, but an exception has been approved by the CISO	Yes				
2	**Is a documented process followed for installing security updates/patches?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Answer Choices:	No documented process exists	Yes, a documented process exists					
3	**How long after a security update is released before the OS is updated?**						
Requirement:	https://it.tamu.edu/cc/CM-1						
Comments:	OS security updates released by the vendor.						
Answer Choices:	Do not update	greater than 60 days	within 60 days	within 30 days	Immediately		
4	**Is whole disk encryption used?**						
Requirement:	https://it.tamu.edu/cc/RA-2						
Comments:	If stolen or lost, whole disk encryption helps protect data stored on the IT resource.						
Answer Choices:	No	Yes					
5	**Is data loss protection (DLP) software used?**						
Requirement:	https://it.tamu.edu/cc/RA-2						
Answer Choices:	No	Yes	Yes, use the university-supplied DLP software				
6	**Is the university-supplied anti-virus/anti-malware installed?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Answer Choices:			No	No, but an exception has been approved by the CISO	Yes		
Next Section:	**Depends on answer choice for question 6.**		**Section 4: Logs (Pg 10)**		**3d: Security Management (Pg 10)**		

Only answer these questions if "Yes" was the answer for question 6 in 3c.

3d: Security Management							
Section comments:	This part of Section 3 follows up on security management.						
1	**Do you make changes to the university-supplied anti-virus/anti-malware to reduce its effectiveness?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Comments:	Changes can include disabling, bypassing, or altering.						
Answer Choices:	No	Yes					
Next Section:	**Section 4: Logs (Pg 10)**						

Only answer these questions if "No" or "No, but an exception has been approved by the CISO" for question 6 in 3c OR if you answered the question in 3d.

Section 4: Logs							
Section comments:	Section 4 focuses on logging requirements for the IT resource. It is broken up into parts based on the answers provided.						
1	**Where are logs stored?**						
Requirement:	https://it.tamu.edu/cc/AU-2						
Comments:	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**	**4a: Logs (Pg 11)**		**4b: Logs (Pg 12)**	

Only answer these questions if "Logs stored locally" or "Logs sent to external server" was the answer for question 1 in Section 4.

4a: Logs							
Section comments:	This part of Section 4 focuses on logging requirements.						
1	**Are the date and time recorded with each logged event?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	Date & Time are not recorded		Date & Time are recorded				
2	**Do logged events include the User IDs (usernames)?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Yes					
3	**Are authentication attempts logged?**						
Requirement:	https://it.tamu.edu/cc/AU-2						
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts				
4	**Are controls in place to prevent the deletion or modification of logs?**						
Requirement:	https://it.tamu.edu/cc/AU-9						
Answer Choices:	Logs are not protected	Logs are protected					
5	**Are logs kept a minimum of 30 days?**						
Requirement:	https://it.tamu.edu/cc/AU-11						
Answer Choices:	No	Yes					
Next Section:	**Done**						

Only answer these questions if "Logs sent to Division of IT Splunk service" was the answer for question 1 in Section 4.

4b: Logs							
Section comments:	This part of Section 4 focuses on logging requirements when logs are sent to the Division of IT Splunk service.						
1	**Are the date and time recorded with each logged event?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	Date & Time are not recorded		Date & Time are recorded				
2	**Do logged events include the User IDs (usernames)?**						
Requirement:	https://it.tamu.edu/cc/AU-3						
Answer Choices:	No	Yes					
3	**Are authentication attempts logged?**						
Requirement:	https://it.tamu.edu/cc/AU-2						
Answer Choices:	No logging	Logs only failed attempts	Logs successful & failed attempts				
Next Section:	**Done**						