The purpose of this document is to walk individuals who solely manage end-user devices (desktops, laptops, tablets, etc.) through the *2021 IT Risk Assessment - End-User Devices* assessment. The layout of the questions is similar to what the individual will see when completing the assessment using the Google Form.

2021 IT Risk Assessment - End-User Devices

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 five 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. You are encouraged to keep the results for your records.

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	**IT resource description:**						
Comments:	Explain what the IT resource 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:**						
Comments:	Select the option that applies to the IT resource.						
Answer Choices:	Desktop / Laptop	Tablet or other mobile device	Other				
f	**Operating system (OS):**						
Comments:	Select the applicable operating system for the IT resource.						
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 IT resource:**						
Comments:	Enter a number (e.g. 1, 2, 3)						
h	**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			
i	**What is the impact level of the IT resource?**						
Comments:	If you are not sure what the IT resource's impact level is, use the impact level calculator in the link below.						
Impact calculator:	https://u.tamu.edu/impactcalc						
Answer Choices:	Low	Moderate	High				

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 selected.				
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	**Is a documented procedure in place to ensure access is limited based on least privilege?**					
Requirement:	https://it.tamu.edu/cc/AC-6					
Comments:	The university employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with university missions and business functions. More information on least privilege can be found in the link below.					
More information:	https://en.wikipedia.org/wiki/Principle_of_least_privilege					
Answer Choices:	No documented procedure exists	Yes, a documented procedure exists				
3	**Have all default passwords been changed (e.g., blank administrator passwords, user ID/passwords that the supplier provided, or that came with the operating system like admin/admin, root/root, or sudo/sudo)?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	Example default passwords: blank administrator passwords, user ID/passwords that the supplier provided for the IT resource, or that came with the IT resource like admin/admin, root/root, or sudo/sudo Many IT resources come with a standard default account that uses the same standard name/password combination across all the IT resources of that type, brand, series, etc. Malicious actors try to gain unauthorized access by using those account credentials.					
Answer Choices:	Default passwords not changed	Default passwords changed	No default accounts exist or accounts with default passwords have been removed			
4	**Do documented procedures exist for changing shared account (root, administrator, etc.) passwords when staff or duties change?**					
Requirement:	https://it.tamu.edu/cc/AC-5					
Answer Choices:	No documented procedure exists	Yes, a documented procedure exists	No shared accounts exist			
5	**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 >30 minutes	Screen lock >15 minutes	Screen lock ≤15 minutes		

6	Does the IT resource use university central authentication (NetID)?						
Comments:	Not referring to default or pre-defined accounts (e.g., the root user in a Linux operating system, local administrator on Windows).						
Website link:	NetID https://infrastructure.tamu.edu/identity/netid.html						
Answer Choices:			No	Yes, but some user accounts do not use NetID	Yes, exclusively NetID		
Next Section:	**Depends on answer choice for question 6.**		**2a: Access Management (Pg. 4)**		**Section 3: Resource Maintenance (Pg. 8)**		

Only answer these questions if "No" or "Yes, but some user accounts do not use NetID" was the answer for question 6 in Section 2.

2a: Access Management							
Section comments:	This part of Section 2 focuses on user account access, authentication systems, etc.						
1	**Are User IDs (usernames) unique?**						
Requirement:	https://it.tamu.edu/cc/AC-2						
Answer Choices:	Users are not identified	Shared IDs are used	Shared & Unique IDs are used	Only Unique IDs are used			
2	**Do any third parties (e.g., research affiliates, business associates, service providers, vendors, contractors) have access to the IT resource?**						
Answer Choices:	No	Yes					
3	**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		

4	**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		
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	**Is multifactor authentication used?**						
Requirement:	https://it.tamu.edu/cc/IA-2						
Comments:	Multifactor authentication adds an extra layer of security. Texas A&M University uses Duo for NetID to meet this requirement.						
Website link:	Duo	https://it.tamu.edu/duo/					
Website link:	NetID	https://infrastructure.tamu.edu/identity/netid.html					
Website link:	CAS	https://infrastructure.tamu.edu/auth/CAS/cas.html					
Answer Choices:	No	Yes, alternate 3rd party tool	Yes, using Duo but not through CAS	Yes, through university CAS authentication			
7	**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 6.**		**2c: No Authentication (Pg. 7)**	**2b: Password Management (Pg. 6)**		**Section 3: Resource Maintenance (Pg. 8)**	

Only answer these questions if "Pin code" or "Passwords" was the answer for question 7 in 2a.

Section 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-5						
Answer Choices:	Allows blank passwords	Allows <8 characters passwords	Requires ≥8 characters	Requires ≥16 character passwords			
2	**What are the minimum password complexity requirements being enforced?**						
Requirement:	https://it.tamu.edu/cc/IA-5						
Comments:	If passwords can be less than 16 characters, then they must contain three of the following four groups of characters: lower case letters, upper case letters, symbols or numbers. If passwords must be at least 16 characters long, then 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 passwords have to be at least 16 characters long, then users are not required to meet the complexity requirements.						
Answer Choices:	No	Yes	At least 16 characters required - no complexity requirement				
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 a login attempt fails, is the user informed of which part of the username/password combination is incorrect?**						
Requirement:	https://it.tamu.edu/cc/IA-6						
Comments:	Failed login boxes/messages after a failure should not indicate which part of the username/password combination is incorrect. Example message: "login and/or password incorrect."						
Answer Choices:	No	Yes					
6	**How many consecutive invalid login 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 attempts				
7	**How long until the IT resource 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	Locked until administrator reset		
Next Section:	**Section 3: Resource Maintenance (Pg. 8)**						

Only answer these questions if "No authentication required" was the answer for question 7 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. 8)**

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 selected.					
1	**Is the installed version of the operating system (OS) officially supported by the vendor?**					
Requirement:	https://it.tamu.edu/cc/SI-3					
Comments:	"Officially supported" means the vendor is still releasing patches/updates. Security patches/updates are important because they fix known weaknesses and vulnerabilities that are used by malicious actors.					
Answer Choices:	No	No, but a current exception request has been approved by the CISO	Yes			
2	**Is a documented process followed for installing security patches/updates?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	The process should cover both the OS level and all installed applications and/or software.					
Answer Choices:	No documented process exists	Yes, security patches/updates are installed using a documented process				
3	**Is the university required schedule for installing OS level security patches being followed?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	OS security patches/updates released by the vendor or development organization. University required schedule: (a) Security patches categorized as "critical" by the vendor = installed within 30 days of release; (b) Security patches categorized as "high" by the vendor = installed within 45 days of release; (c) Other security patches = installed within 60 days of release.					
Answer Choices:	No	No, but a current exception request has been approved by the CISO	Yes			
4	**Is all 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				

5	**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					
Comments:	"Unsupported" means the vendor is no longer releasing patches/updates. Unsupported software not only leaves you and the university open to security risks but may cause other issues as software and hardware may stop working or be incompatible with newer systems.					
Answer Choices:	No	Yes, but a current exception request has been approved by the CISO	Yes			
6	**Is the university required schedule for installing security patches being followed for all installed software and/or applications?**					
Requirement:	https://it.tamu.edu/cc/CM-1					
Comments:	Security updates for applications and/or software are released by the various vendors or development organizations. University required schedule: (a) Security patches categorized as "critical" by the vendor = installed within 30 days of release; (b) Security patches categorized as "high" by the vendor = installed within 45 days of release; (c) Other security patches = installed within 60 days of release.					
Answer Choices:	No	No, but a current exception request has been approved by the CISO	Yes			
7	**Is there a procedure in place to ensure the storage media related to the IT resource is properly sanitized prior to disposal and/or release from your control?**					
Requirement:	https://it.tamu.edu/cc/MP-6					
Comments:	Storage media may include internal or external hard drives.					
Answer Choices:	No documented procedure exists	Yes, a documented procedure exists				
8	**Is whole disk encryption used?**					
Requirement:	https://it.tamu.edu/cc/RA-2					
Comments:	If stolen or lost, whole disk encryption helps prevent the data stored on the IT resource from being easily accessible/read.					
Answer Choices:	No	Yes				

9	When was the last vulnerability scan?						
Requirement:	https://it.tamu.edu/cc/RA-5						
Answer Choices:	Never scanned	Scanned >12 months ago	Scanned <12 months ago	Scanned <6 months ago			
10	**Is the university-supplied data loss prevention (DLP) software installed?**						
Requirement:	https://it.tamu.edu/cc/RA-2						
Comments:	Spirion is the university-supplied data lost prevention (DLP) software. Talk to your unit IT staff as they will be the ones that work with you to install it on the IT resource.						
Answer Choices:	No	No, but a current exception request has been approved by the CISO		Yes			
11	**Is the university-supplied anti-virus/anti-malware installed?**						
Requirement:	https://it.tamu.edu/cc/SI-3						
Comments:	CrowdStrike Falcon is the university-supplied anti-virus/anti-malware. This can only be provided to System part 02 members. Talk to your unit IT staff as they will be the ones that work with you to install it on the IT resource.						
Answer Choices:			No	No, but a current exception request has been approved by the CISO		Yes	
Next Section:	**Depends on answer choice for question 9.**		**Section 4: Backups (Pg. 11)**			**3a: Security Management (Pg. 10)**	

Only answer this question if "Yes" was the answer for question 9 in Section 3.

3a: 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: Backups (Pg. 11)**						

These questions must always be answered.

Section 4: Backups							
Section comments:	Section 4 focuses on data backup requirements for the IT resource. It is broken up into parts based on the answers selected.						
1	**Are data backups performed?**						
Requirement:	https://it.tamu.edu/cc/CP-9						
Comments:	Backups help prevent data from being lost if the primary storage media has been corrupted and/or stolen.						
Answer Choices:			No	Yes			
Next Section:	**Depends on answer choice for question 1.**		**Section 5: Logs (Pg. 12)**	**4a: Backups (Pg. 11)**			

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

4a: Backups							
Section comments:	This part of Section 4 focuses on data backup requirements.						
1	**How often are data backups performed?**						
Requirement:	https://it.tamu.edu/cc/CP-9						
Answer Choices:	Ad hoc backups performed	Scheduled monthly backups performed	Scheduled weekly backups performed	Scheduled daily backups performed			
2	**Are the backup media encrypted?**						
Requirement:	https://it.tamu.edu/cc/CP-9						
Answer Choices:	No	Yes	Not required, no Confidential (or higher) data				
Next Section:	**Section 5: Logs (Pg. 12)**						

These questions must always be answered.

Section 5: Logs						
Section comments:	Section 5 focuses on logging requirements for the IT resource. It is broken up into parts based on the answers selected.					
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**	**5a: Logs (Pg. 12)**		**5b: Logs (Pg. 13)**

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

5a: Logs						
Section comments:	This part of Section 5 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	How are logs monitored?						
Requirement:	https://it.tamu.edu/cc/AU-2						
Comments:	Reviewing logs manually or with the use of a tool, is a proactive measure administrators can take to help detect possible security threats or issues that impact the performance or security of the IT resource.						
Answer Choices:	Logs are never reviewed	Manually on an ad hoc basis	Manually on a regular schedule	Real-time using automated systems			
5	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					
6	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 5.

5b: Logs						
Section comments:	This part of Section 5 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					