Area of Responsibility:	Information Technology
Responsible Contact:	Chief Information Officer
Policy Identification:	Cybersecurity Policy
Effective Date:	07/21/2021
Last Revised:	04/26/2022

POLICY

Virginia Union University is committed to safeguarding the confidentiality, integrity, and availability of all physical and electronic information assets to ensure that regulatory, operational and contractual requirements are fulfilled.

This policy establishes people, process, and technology-based requirements to protect the confidentiality, integrity and availability and reliability of Virginia Union University ’s information and resources.

The overall goals for cyber security at Virginia Union University are the following:

1. Comply with requirements for confidentiality, integrity, and availability for Virginia Union University ' information assets and services.
2. Comply with industry best practices at the program, process, and system levels in accordance with the guidance set forth in this policy.
3. Ensure that Virginia Union University is capable of continuing operations even if major security incidents occur.
4. Ensure that third party suppliers comply with Virginia Union University' information security requirements.
5. Establish controls for protecting Virginia Union University' information and information systems against theft, abuse and other forms of harm and loss.
6. Establish requirements for controlling access to all Virginia Union University information assets, including computer and communication systems.
7. Establish a framework to define administrator and employee responsibilities for information security.

The following industry frameworks, leading practices and regulatory requirements are leveraged to help ensure comprehensive coverage and alignment of Virginia Union University’ security controls:

NIST CSF: NIST Cyber Security Framework is risk-based approach to managing cybersecurity risk. The Framework Core consists of functions, which organize all cybersecurity activities into 5 groups - Identify, Protect, Detect, Respond and Recover.

This policy applies to all users of Virginia Union University Information Resources.

Key Cyber Security Policies

Virginia Union University has five key cyber security policies, specifically:

1. Acceptable Use of Information Resources
2. Data Governance Policy
3. Identity and Access Management Policy
4. System and Device Security Policy
5. Network Security Policy

Processes and Procedures – IT Controls

IT is responsible for IT controls including processes and procedures.

Security Exceptions

When the cyber security policies or IT controls are not met, a security exception must be requested. Prior to submitting a security exception, it is important to work cyber security to explore solutions that are compliant and meet your need.

The following information is required for exception requests:

1. Applicable Security Standard/Procedure/Baseline (Please specify to which security standard, procedure or baseline this service does not comply.)
2. Gap or missing control (Please specify the security control to which the service in question does not comply.)
3. Associated environment impacted by the gap (Please describe the environment associated with the gap noted above. Include any related documentation or links.)
4. Reason for non-compliance (What is the reason/root cause for non-compliance?)
5. Business impact if not approved (Please elaborate as to why it is important for the business to continue in a non-compliant manner. Provide a concise description of any business impacts (such as users affected, legal or contractual issues, deliverables etc.) and costs that the business will experience if the exception is not approved
6. Remediation Plan (Please detail the plan to remediate the non-compliance)
7. Remediation Timeline (Please specify the date when you anticipate having the item of non- compliance remediated.)
8. After you have gathered the necessary information, submit the security exception for review and possible approval by emailing the Senior IT Director. All exception requests will be evaluated within 10 business days.

SUPPORTING DOCUMENTS (if applicable)

GLOSSARY

Document Approvals:

_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**