 <b>Office of Credit Unions</b> <b>Policies and Procedures</b>	<b>POLICY NUMBER</b>
	<b>10640</b>
<b>EXAMINATION</b>	<b>EFFECTIVE DATE</b>
	<b>11/01/2018</b>
<b>SUBJECT</b>	<b>REVISION DATE</b>
	<b>04/26/2023</b>
<b>CyberSecurity</b>	<b>PAGE(S)</b>
	<b>Page 1 of 2</b>

## I. PURPOSE

Cybersecurity is the process of protecting consumer and financial institution information by preventing, detecting, and responding to attacks. An effective cybersecurity program must include satisfactory identification and management of internal and external threats and vulnerabilities, implementation of appropriate controls and monitoring systems, and periodic controls testing. Examiners must assess management’s oversight, policies and procedures regarding cybersecurity. Considering the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution’s overall information security program.


It is essential for management to adequately prepare for and respond to cybersecurity events. Inadequate or untimely responses to cybersecurity incidents can erode public confidence and negatively impact the safety and soundness of the financial institution. Management should take a comprehensive approach in maintaining the security and resilience of its technology infrastructure through the establishment of a robust cybersecurity framework.

## II. PRIMARY REFERENCES / GUIDANCE

1. [FFIEC Cybersecurity Assessment Tool](#)
2. [FFIEC Information Technology Examination Handbook](#)
3. [NIST Cybersecurity Framework](#)
4. [CISA Shields Up!](#)
5. [NCUA Automated Cybersecurity Evaluation Toolbox \(ACET\)](#)

## III. BACKGROUND

Financial institutions are increasingly dependent on information technology and telecommunications to deliver services to consumers and businesses every day. Disruption, degradation, or unauthorized alteration of information and systems that support these services can affect operations and core processes and undermine confidence in the nation’s financial services sector.

 <b>Office of Credit Unions</b> <b>Policies and Procedures</b>	<b>POLICY NUMBER</b>
	<b>10640</b>
<b>EXAMINATION</b>	<b>EFFECTIVE DATE</b>
	<b>11/01/2018</b>
<b>SUBJECT</b>	<b>REVISION DATE</b>
	<b>04/26/2023</b>
<b>CyberSecurity</b>	<b>PAGE(S)</b>
	<b>Page 2 of 2</b>

Cyber incidents can have financial, operational, legal, and reputational impact on a financial institution. Costs may include forensic evaluations, public relations campaigns, legal fees, consumer credit monitoring and technology changes. Cybersecurity needs to be integrated throughout an institution as part of an institution-wide governance process, including information security, business continuity, third-party risk management and audit.

To assist regulators and financial institutions in assessing and rating cybersecurity preparedness and effectiveness, a Cybersecurity Assessment Tool (CAT) is available through the FFIEC and NCUA. While the use of these tools is not required, each institution should develop procedures to regularly review and evaluate the effectiveness of the institution’s cybersecurity program.

#### **IV. MINIMUM PROCEDURES**

1. Review the institution’s products, services, information systems, and reliance on third-party servicers to determine the overall cyber risk.
2. Assess management’s preparedness to address and respond to cyber issues.
3. Review the institution’s procedures and preparedness for a cyber issue in relation to the institution’s inherent risks.
4. Review the institution’s evaluation and oversight of third-party service providers.
5. Review and evaluate the institution’s response program to a cyber issue.
6. Review and evaluate the effectiveness of the institution’s cybersecurity audit and testing program, including detection and response capabilities.