

Credit Union

Sample Template for Developing An Information Security Program

See ii Release 0155 and its Exhibits for additional guidance. (NCUA R&R Part 748)

Assess Risk					Manage and Control Risk			Test Controls		Make Adjustments
Information and Information & Systems	Threats and Vulnerabilities	Likelihood	Potential Damage	Risk Rating	Controls	Person Responsible for Controls	Staff Training for the Controls	Person Responsible for Testing/ Frequency	Test Results	Adjust Program after Evaluating Test Results
Identify information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Address both paper-based and electronic. Keep in mind how the CU uses information day-to-day. Address employee access, use, and dissemination of information in response to requests. Consider how you : - store, transmit, transfer, and dispose of media (paper or electronic) containing information, - authorize and authenticate those who receive information both physically and electronically, and - how you make information available for viewing. Add additional topics as needed!	Identify reasonably foreseeable internal and external threats that could result in: • unauthorized disclosure, • misuse, • alteration, or • destruction of member information or member information systems due to environmental hazards, such as fire and water damage or technical failures.	Assess the likelihood of the threat.	Assess the potential damage of the threats, taking into consider-ation the sensitivity of the member information.	Assign a risk rating based on the assessments of likelihood and potential damage, using "High," "Low," or "Medium."	Consider which of the security measures in List A are appropriate for the credit union to manage and control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the credit union's activities.		Train staff to implement the credit union's information security program.	Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs. Regularly test the key controls, systems and procedures of the information security program, with the frequency and nature determined by the credit union's risk assessment.		Monitor, evaluate, and adjust the information security program , as appropriate, the information security program in light of: - changes in technology, - sensitivity of member information, - internal or external threats to information, and - the credit union's own changing business arrangements, such as -- mergers and acquisitions, -- alliances and joint ventures, -- outsourcing arrangements, and -- changes to member information systems.
Data processing system										
CU website										
Home banking										
Bill payment service										
Debit cards										
Credit cards										
Personal computers										
Internet										
Passwords										
Oral conversations										
Telephone conversations										
Telephone communications lines & equipment										

Assess Risk					Manage and Control Risk			Test Controls		Make Adjustments
Information and Information & Systems	Threats and Vulnerabilities	Likelihood	Potential Damage	Risk Rating	Controls	Person Responsible for Controls	Staff Training for the Controls	Person Responsible for Testing/ Frequency	Test Results	Adjust Program after Evaluating Test Results
Vendors - list each handling member data (website & email hosts, firewalls, E-statements, credit reporting, home banking, credit card processing, online loan applications, debit card processing, collection agencies, wire transfers, bill payment, check printing, telephone banking, disaster recovery)										
Paper documents - Account cards, loan docs, etc. - incoming mail - outgoing mail - waste documents - etc.										
Data files - on disks - on drives - in email files										
Information disposal - Paper documents - Electronic media										
Email										
Building access										
Data in storage										
Janitorial, maintenance, contractors										
Backup data										
Couriers										
ATMs										
Employees, officers										
ATMs										
Shared service centers										
Add Additional Topics As Needed										

