Cybersecurity Awareness Training

C.M.M.C. Compliance Support Matrix

Domain	ID	Practice	Applicable Training Element That Supports Compliance
AC	3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Things You Can Do
AC	3.1.20	Verify and control/limit connections to and use of external information systems.	Things You Can Do
AC	3.1.22	Control information posted or processed on Publicly accessible information systems	Things You Can Do
AC	3.1.9	Provide privacy and security notices consistent when applicable CUI rules	Things You Can Do
AC	3.1.21	Limit use of portable storage devices on external systems.	Things You Can Do
AC	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Things You Can Do
AC	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Things You Can Do
AU	3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Things You Can Do
AT	3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risk associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems	Entire Training
AT	3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties.	Entire Training
AT	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	What To Do If You Are Attacked
CM	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Things You Can Do
CM	3.4.9	Control and monitor user-installed software.	Things You Can Do
CM	3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Things You Can Do
IA	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Things You Can Do
IA	3.5.8	Prohibit password reuse for a specified number of generations.	Things You Can Do
IA	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts	Things You Can Do
IA	3.5.6	Disable identifiers after a defined period of inactivity	Things You Can Do

FIREWATER ADVISORS

Cybersecurity Awareness Training

C.M.M.C. Compliance Support Matrix

Domain	ID	Practice	Applicable Training Element That Supports Compliance
IR	3.6.1	Establish an operational incident-handling capability for organizational systems that includes prepartation, detection, analysis, containment, recovery, and user response activities.	What To Do If You Are Attacked
MA	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Things You Can Do
MP	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Things You Can Do
MP	3.8.6	Portable Storage Encryption: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Things You Can Do
PS	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	Things You Can Do
PE	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Things You Can Do
PE	3.10.3	Escort visitors and monitor visitor activity.	Things You Can Do
PE	3.10.4	Maintain audit logs of physical access.	Things You Can Do
PE	3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	Things You Can Do
RE	3.13.1	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	Things You Can Do
SC	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Things You Can Do
SC	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Things You Can Do
SI	3.14.7	Identify unauthorized use of the organizational system.	What To Do If You Are Attacked