PTAC Del Mar College

PTAC at Del Mar College does not promote or endorse any of the products, providers or solutions to obtain CMMC certification.
They are provided for illustrative purposes only.

Cybersecurity Maturity Model Certification (CMMC) Readiness Review Level 1

More in-depth information at https://projectspectrum.io/#!/cmmc/domain/SI.

Access Control -- limit logical access to authorized users only.

ARE YOU CMMC READY?

Establish system access requirements:

☐ Yes ☐ No

Control who uses computers and can log on to your network, deny unauthorized users and devices access. Limit services and devices that can be accessed.

Suggestions:

⇒ Use password manager (Last Pass, 1 Password, Dashlane)
⇒ Train employees annually on basic cyber hygiene

Control internal system access:

☐ Yes ☐ No

Limit users/employees to only those information systems, roles or applications they are allowed and needed to do their jobs.

Suggestions:

⇒ User rights ⇒ Use cloud-based storage/solutions when possible

Limit data access to authorized users & processes:

☐ Yes ☐ No

Control, manage connections between your company & outside networks especially public internet. Be aware of applications run by outside systems. Control, limit personal devices from accessing company network and information. Do not allow sensitive information like FCI and CUI to become public. Know who has access to publish information on public systems like your company website, limit and control information posted on it.

Suggestions:

⇒ Generic e-mail addresses not allowed (G-mail, Hotmail, Yahoo, etc.)
⇒ Website development, hosting not allowed from retail providers (Go Daddy, Host Alligator)

Identification & Authentication -- Ensure any user who tries accessing your system is positively authenticated.

ARE YOU CMMC READY?

Grant access to authenticated entities:

☐ Yes ☐ No

Assign individual, unique identifiers to anyone or devices that accesses your system; confirm those identities before allowing access. Before access is granted, first verify the user or device.

Suggestions:

⇒ Assign user names and passwords.
⇒ Change default, manufacturer-assigned user names and passwords immediately.

Media Protection -- Protect your system against portable devices.

ARE YOU CMMC READY?

Sanitize media:

☐ Yes ☐ No

Any media containing FCI needs to be cleaned, purged, shred or destroyed so it cannot be read. Same applies to paper, files or any other media with this information.

Resource: NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization

Suggestions:

⇒ Routine, regular system & file back-ups
⇒ Develop practices to safeguard: personal identifying, payment card, business, financial information, and intellectual property

Physical Protection -- Limit physical access to information & IT assets.

ARE YOU CMMC READY?

Limit physical access:

☐ Yes ☐ No

Monitor, limit who can enter any areas needing protection. Visitors are not allowed access without an escort. All non-employees need to wear visitor badges or escorted at all times. Keep a record of who accesses your facility and equipment.

Suggestions:

- ⇒ Badges
- ⇒ Key cards
- ⇒ Locked doors
- ⇒ Visitor's log
- ⇒ Employee sign-in log

System & Communication Protection -- provide multi-layer protection to all lines of internal and external communication.

ARE YOU CMMC READY?

Control communication at system boundaries:

☐ Yes ☐ No

Protect your network or system boundaries. Consider separating, monitoring, controlling or protecting one part of your company's enterprise/network from the other. Separate publicly accessible systems from internal ones needing to be protected. Do not place internal systems on the same network as those that are publicly accessible.

Suggestions:

- ⇒ Web proxy
- ⇒ Firewall
- ⇒ Separate network infrastructure
- ⇒ Gateway
- ⇒ Access controls
- ⇒ Subnet
- ⇒ Router
- ⇒ Remove employee access immediately after employment
- ⇒ DMZ: host, part of network put in a neutral zone between internal network & larger one
- ⇒ Dedicate network equipment with separate LAN router

System & Information Integrity -- Recognize alerts and notifications of possible threats, mitigate risks quickly.

ARE YOU CMMC READY?

☐ Yes ☐ No

Identify & manage information system flaws.

Suggestions:

- ⇒ Office 365
- ⇒ Windows 10 Pro
- ⇒ Google G Suite for Business
- ⇒ Two-factor authentication (2FA)

☐ Yes ☐ No

Software updates.

Suggestions:

- ⇒ Purchase support
- ⇒ Patch management process
- ⇒ Be on lookout for newsletters, updates (common problems, weaknesses)

☐ Yes ☐ No

Identify malicious content:

Stop malicious code at designated system locations, have a plan how often to conduct scans.

Suggestions:

- ⇒ Anti-virus software
- ⇒ Anti-malware software
- ⇒ Enter web address into browser, not internet search
- ⇒ Stay current with system updates, security releases
- ⇒ Routinely scan for viruses
- ⇒ Do not click on unrecognized e-mails, links, attachments