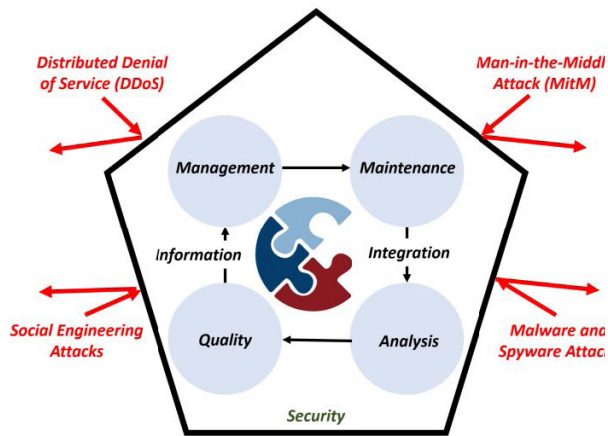


Cyber Security

“If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people’s accounts. If they know there’s a key hidden somewhere, they won’t stop until they find it.”

- Tim Cook



Information is among an organization’s most valuable assets. Accordant Federal optimizes information management, maintenance, analysis, and security—ensuring integration at all organizational levels.

Information excellence is of little value if the information is compromised. Systems integration becomes a liability if it grants hackers access to all levels of the enterprise. Accordant Federal’s cyber security solutions are designed to isolate and neutralize cyber threats. Government customers are at the highest risk of cyber infiltration. Acts of espionage often begin on less secure networks and, through compromised access protocols, escalate to protected network architectures.

Accordant’s cyber security offering protects mission objectives from compromise. This is accomplished by securing access and integrating systems in accordance with the following principles:

- 1. Confidentiality.** Data segmentation protects information by ensuring it is accessed only by those

who require it. Accordant works with partners to implement data silos that keep confidential information limited to those granted specific access. Multi-layer verification of credentials prevents infiltration.

- 2. Integrity.** Accordant ensures infiltrators and other unauthorized parties do not modify or delete data. Through constant backup, regular audits, and encryption, Accordant helps preserve the hygiene and accuracy of information used to achieve mission objectives.
- 3. Availability.** Information drives every action in complex problem solving. Without reliable access to required data, your team members cannot do their jobs. Accordant works with partners to introduce redundant networks, servers, and applications across the enterprise. These measures enhance data availability - even during natural disasters and other crisis scenarios.

“Cyber criminals can use personal details, such as your favorite color, the last four digits of your credit card and your email addresses, to make educated guesses about your sign-in credentials.”

- Larry Alton

By implementing repulsive security measures that intercept and neutralize all forms of cyber attack, Accordant can protect your technological gates from internet barbarians. Accordant cyber defense measures protect partners from a multitude of threats; including:

- 1. Distributive Denial of Service (DDoS)**—One of the most powerful weapons at a hacker’s disposal, a DDoS attack overwhelms a networked asset with more traffic than it can handle, rendering it inoperable.
- 2. Man-in-the-Middle Attack (MitM)**—The technological equivalent to eavesdropping, MitM attacks allow hackers to monitor communications between legitimate users.
- 3. Social Engineering Attacks**—Relying on psychological manipulation, social engineering attacks extract sensitive information from unsuspecting users.
- 4. Malware and Spyware Attacks**—Malicious software is a threat to every organization. When unsuspecting team members expose themselves to predatory material, the network is compromised.

Information Management Solutions



ACCORDANT FEDERAL, LLC

7902 Tysons One Place, Suite 715
Tysons Corner, VA 22102

Ph: (610) 823-2123

Jeff@AccordantFederal.com | www.AccordantFederal.com