12 Pillars of Cybersecurity

Disaster Recovery

Ensures organizations can restore systems and data quickly after disruptions such as ransomware, hardware failures, or natural disasters.

Authentication

Verifies user identity using strong passwords, secure login controls and MFA to prevent unauthorized access.

Authorization

Controls what users can access by enforcing least■privilege principles and role■based access rights.

Encryption

Protects sensitive data at rest and in transit by making it unreadable to unauthorized users.

Vulnerability Management

Identifies and remediates system weaknesses before attackers can exploit them.

Audit & Compliance

Monitors controls to ensure alignment with legal, industry and organizational security requirements.

Network Security

Secures network traffic through protections such as segmentation, DNS security and firewalls.

Terminal / Endpoint Security

Protects endpoints like laptops and mobile devices using security tools such as EDR and endpoint encryption.

Emergency Response

Enables rapid detection, response and recovery in the event of an active cyber incident.

Container Security

Secures applications deployed using containers by protecting images, configurations and runtime behavior.

API Security

Secures data flow between systems by protecting APIs from unauthorized access and abuse.

Third■Party / Vendor Management

Reduces external risk by assessing and monitoring vendors that interact with the organization’s systems.

Contact DISC InfoSec: info@deurainfosec.com