Blue Stripe Tech IT Security Policies

DoD Cybersecurity Compliance & Framework

JACINTA IZUNDU

PURPOSE

The purpose of these IT security policies is to align Blue Stripe Tech’s IT infrastructure and project services with U.S. Air Force cybersecurity requirements while guiding users in understanding and complying with Department of Defense regulations related to governmental contracts. By adhering to these regulations, the policies aim to establish a robust IT security framework that supports effective project execution.

BLUE STRIPE

BACKGROUND

Blue Stripe Tech has been awarded a project for the U.S. Air Force Cyber Security Center (AFCSC). Compliance with DoD standards and IT security policies is important, because winning this project increases the service provider’s revenue by 30%. The DoD specific policies, compliance requirements, and IT infrastructure standards necessary to align with the project’s requirements are mentioned below.

MAIN SECURITY

FRAMEWORK WE USE

These frameworks guide how we protect information and manage risks.
They ensure we meet the security standards expected by the Department of Defense

- NIST 800-171: Protects sensitive data (CUI)
- CMMC 2.0: DoD security maturity requirements
- DoD Risk Management Framework: Helps manage risks and controls

EMPRESA ENSIGNA

USER SECURITY (EMPLOYEES)

Policies:

- Strong password + Multi-Factor Authentication (MFA)
- Give people only the access they need
- Provide security training

Controls:

- Review access logs
- Disable inactive accounts

we protect accounts by using strong passwords, MFA, and limiting access only to what employees need.
Regular monoitoring ensures no unauthorized useres get into our systems

WORKSTATION SECURITY (LAPTOPS & DESKTOPS)

Policies:

- Install antivirus/endpoint protection
- Regular software updates
- Limit admin rights

Controls:

- Encrypted storage
- Block unauthorized USB devices

We secure all company devices by using antivirus tools, installing updates, and limiting admin rights. This helps prevent malware, hacking, and data leaks from employee computers.

INTERNAL NETWORK SECURITY (LAN)

Policies:

- Use firewalls and IDS/IPS
- Separate sensitive systems (network segmentation)

Controls:

- Monitor traffic 24/7
- Alert on unauthorized access attempts

Firewalls and IDS/IPS help us detect and block suspicious traffic inside the company network.
Network segmentation isolates sensitive systems so attacks cannot spread easily.

INTERNET SECURITY (LAN-TO-WAN)

Policies:

- Encrypt all internet traffic (HTTPS, VPN)
- Use web filters to block harmful sites

Controls:

- Scan web traffic
- Review firewall rules regularly

We encrypt internet traffic and use VPNs to keep data safe while moving in and out of the company.
Web filters and secure gateways block dangerous websites and online threats.

EXTERNAL NETWORK (WAN)

All external connections are protected using advanced threat detection tools. Regular audits help us identify weak points and improve network defenses.

POLICIES

- Use advanced threat protection
- Have backup connections for reliability

CONTROLS

- Auto-block unauthorization
- Monthly security audits

REMOTE ACCESS SECURITY

Remote workers must use secure VPN connections and MFA to access company systems.
Monitoring these sessions ensures personal devices or unauthorized users cannot get in.

POLICIES

- Require VPN + MFA for working remotely
- No personal devices allowed

CONTROLS

- Log and monitor remote sessions
- Report failed login attempts

SYSTEM & APPLICATIONS

We secure servers, applications, and email by encrypting data and performing regular security tests.
Log reviews and penetration testing help us detect weaknesses before attackers do.

POLICIES

- Encrypt data and secure backups
- Protect email from phishing

CONTROLS

- Keep audit logs
- Do yearly penetration tests

SUMMARY

Blue Stripe Tech Ensures DoD Compliances by:

- Securing users, devices, networkd and sytems
- Following strict DoD frameworks
- Monitoring and protecting all activities
- Reducing risks through strong policies and controls

THANK YOU

+1 -217-670-4436

clemsjacy@gmail.com

http://linkedin.com/in/jacinta-izundu-b36a20233