Blue Stripe Tech

Department of Defense Ready

Burhan Khan

Blue Strip Tech – IT Services Provider

Table of Contents

[Part 1 – US Compliance Laws Research 3](#_Toc100574043)

[Part 2 – Infrastructure Research A 5](#_Toc100574044)

[Security Framework 5](#_Toc100574045)

[Policies 6](#_Toc100574046)

[Policy 1 - Mandatory Access Controls 6](#_Toc100574047)

[Termination- Policy 2 6](#_Toc100574048)

[Personnel Security- Policy 3 6](#_Toc100574049)

[Configuration Management- Policy 4 6](#_Toc100574050)

[Awareness And Training- Policy 5 8](#_Toc100574051)

[Audit And Accountability- Policy 6 9](#_Toc100574052)

[Contingency Planning- Policy 7 10](#_Toc100574053)

[Identification and Authentication- Policy 8 11](#_Toc100574054)

[Incident Response- Policy 9 12](#_Toc100574055)

[Maintenance- Policy 10 12](#_Toc100574056)

[Standards 13](#_Toc100574057)

[Accounts- Standard 1 13](#_Toc100574058)

[Infrastructure Standard- 2 13](#_Toc100574059)

[Support Standard- 3 14](#_Toc100574060)

[User Domain 14](#_Toc100574061)

[Controls for User Domain 14](#_Toc100574062)

[Workstation Domain 15](#_Toc100574063)

[Controls for Workstation Domain 15](#_Toc100574064)

[LAN Domain 15](#_Toc100574065)

[Controls for LAN Domain 15](#_Toc100574066)

[LAN to WAN Domain 16](#_Toc100574067)

[Controls for LAN to WAN Domain 16](#_Toc100574068)

[Part 3 – Infrastructure Research B 16](#_Toc100574069)

[WAN Domain 16](#_Toc100574070)

[Controls for WAN Domain 16](#_Toc100574071)

[Remote Access Domain 17](#_Toc100574072)

[Controls for Remote Access Domain 17](#_Toc100574073)

[Systems/Applications Domain 17](#_Toc100574074)

[Controls for Systems/Applications Domain 17](#_Toc100574075)

[Part 4 – Conclusions and Outcomes of Overall Report 18](#_Toc100574076)

[References 19](#_Toc100574077)

# Part 1 – US Compliance Laws Research

While conducting research for US compliance laws I have found that many compliance laws exist for different industries in order to safeguard themselves in cyber space. Organizations are facing an ever-increasing list of regulatory, contractual, and legal compliance obligations. The department of Defense has compliance laws in place for contractors such as DFARS (Defense Federal Acquisition Regulation Supplement). This is meant to ensure that contractors maintain cybersecurity guidelines put in place by the National Institute of Stands and Technology specifically NIST SP 800-171. It is crucial that our organization Blue Stripe Tech pays close attention to this specific government regulation since we are a DoD contractor.

To effectively meet minimum requirements put forth by the DoD contractors like us must ensure adequate security and rapidly report cyber incidents. This may sound straight forward but is complex when put in practice. This is due to the ever-growing list of policies, procedures, and technologies a modern organization must have in place. Contractors must pass a readiness assessment following NIST SP 800-171. While conducting research I have stumbled upon Public Law 113-282. The purpose of this is to provide a comprehensive framework for ensuring the effectiveness of cyber security controls over information resources that support Federal operations and assets. Department of Defense contractors must follow DFARS to remain compliant in the following 14 areas such as Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection, lastly System and information integrity. Under each of these 14 categories there are 110 specific requirements that must be met. For example, under Identification and Authentication there are 11 requirements that consist of aspects like using multifactor authentication for local and network access, employing replay-resistant authentication mechanisms for access to networked recourses, Storing and transmitting only encrypted passwords.

NIST has three links for guidance to help business comply with federal government security requirements. NIST handbook 162 provides a guide to assess a manufacturers information system against the security requirements in NIST SP 800-171. NIST currently has Cyber Security guidelines for DoD contractors that process, store, or transmit controlled unclassified information. The Federal Information Security Management Act was passed in 2002 and is a United States Federal law. It requires government agencies to implement information security programs to ensure confidentiality, integrity, and availability of their information systems. This law also includes IT systems that are provided or managed by contractors.

Implementing policies to remain FISMA compliant could be of great importance to our organization since we are a federal contractor. FISMA provides the foundation to protecting an organization from unauthorized access, use, disclosure, disruption, or modification of information. Organizations who are partnered with the government and receive a low FISMA score could lose any future government contractors. To prevent this from happening to us FISMA frameworks could be a potential solution to us. Other compliance laws that have been put in place in recent times are CMMC (Cyber Security Maturity Model Certification) program. This requires that contactors have the have this certification level from an approved auditor before being given a government contract.

There a specific compliance laws that exists for cloud computing. At Blue Stripe Tech if we ever offer cloud consulting services we should remain mindful of obligation that we will be held accountable for. One such government program that is currently in existence for government contractors is the Federal Risk and Authorization Management Program (FedRAMP). The office of Management and Budget released this to provide a cost effective, risk-based approach for IT infrastructure. Contractors that provide cloud computing services to the U.S. government must prove compliance with this program. FedRAMP has been put in place so that organization can leverage from the cloud, but remain mindful of security. FedRAMP offers 3 impact levels to categorize your security posture.

# Part 2 – Infrastructure Research A

## Security Framework

Our goal is to protect the organization by strengthening security and privacy. To achieve our mission of protecting the organization our security team finds that NIST 800-53 provides the most comprehensive security policy framework to protect the organization from a broad range of threats and risks. NIST 800-53 provides a catalog of security and privacy controls for information systems and organizations to protect company assets, individuals, and the nation from a diverse set of threats and risks such as hostile attacks, human errors, natural disasters, structural failures, foreign intelligence, and privacy risks.

Preventing Blue Stripe Tech from financial losses due to not being DoD compliant is our ultimate mission this is why we chose NIST 800-53 as it seeks mainly to increase the security of information systems used by the federal government. NIST 800-53 will give us the guidelines to protect our User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domains, WAN domain, Remote Access Domain, and System/Application Domains.

## Policies

### Policy 1 - Mandatory Access Controls

A mandatory access control policy will allow the organization to leverage software that applies a uniformly enforced policy across all users to determine who can do what. Just by enforcing access controls within all systems we can achieve confidentiality, integrity, and availably.

### Termination- Policy 2

Any employee that leaves the company or is terminated will notify IT immediately so that they can disable the employee’s account. It is crucial that our organization follows this policy as it will allow us to protect sensitive information from unauthorized access. Failure in not complying with this policy could potentially result in unauthorized data modification or destruction, leaving the business at risk.

### Personnel Security- Policy 3

To protect our organization, we must ensure personnel security is considered. We will not allow anyone inside the building to enter without a company issued key-tag. The IT department will be given the authority to limit these key-tags to only be effective during business hours. Should access be needed outside of business hours then you must contact IT immediately. All employees must undergo a background check before being hired.

### Configuration Management- Policy 4

The following is a collection of activities focused on establishing and maintaining the integrity of information technology infrastructure through proper configuration, management, and monitoring.

* All devices will be deployed with the least amount of functionality
* Shut down any unnecessary ports and services. We can always add functionality on top of the system if needed. Principle of least functionality allows us to limit our attack surface by only deploying what we need
* Deploy Anti-Virus
* No machine should be allowed to go into production without anti-virus. Anti-Virus allows us to remain protected against known threats.
* Deploy SIEM
* All company owned devices be it laptops or web servers will have a security information event management tool deployed on them for continuous monitoring of anything suspicious that may occur. An SIEM will allow the security team to remain proactive instead of reactive.
* MFA On All Accounts
* Having Multi factor authentication enabled on all user accounts allows us to add an extra layer of security by having the user approve the login. Effectively enabling MFA will allow our organization to know that a person is who they say they are before being granted access to company systems.
* Updates
* Updates will be approved on our WSUS server every 3 months to ensure all machines are receiving the updates. This will allow us to have the latest security patches
* Enable Logging on All Devices
* Having logging enabled will allow us to track unauthorized access of systems and determine the root cause if a failure occurs. Logging will also help the security team in efficiently doing an audit.
* Deploy Firewall
* Deploying a firewall will allow for us to block unwanted coming into and going out of our network. Having a firewall in place will also allow us to use a VPN to secure communications coming into and going out of our network.
* Block all outbound connections
* Deny ports 67, 68 going from outside the LAN to the WAN to ensure protection against known malware
* Block all freeware sites due to their historical affiliation with malware
* Email Filter Mimecast
* We will use Mimecast to ensure emails are kept for our records with a duration of at least 10 years
* All spam protections will be enabled
* Sandboxing will be enabled to protect from malicious attachments

### Awareness And Training- Policy 5

Awareness and Training is an important factor in any security program to ensure employees are aware of company policies and procedures.

* Provide a basic security training annually for the entire company
* Annual training will allow for a fresh reminder on company policies
* Provide Role Based Training
* An employee in a new role should be given proper training and should be made aware of the importance of the information they will be handling in their current role or new role.
* Test Effectiveness of Training
* The IT department will send out a phishing email or has the right to simulate any other attack after training to ensure the organizations readiness in the event of a catastrophe

### Audit And Accountability- Policy 6

The goal of this policy is to ensure proper tracking of IT systems to ensure the over-all architecture is being maintained, no unknown devices are on company networks, that the infrastructure is free of unauthorized access, and free of security bugs.

* Run a network scan quarterly
* This is to ensure no unknown devices exists on our corporate networks
* Review the SIEM tool quarterly
* Quarterly review of the SIEM tool allows the security team to properly track devices and events
* All devices will have logging enabled a quarterly review of all logs aggerated by the SIEM tool will be reviewed to ensure no suspicious activity has occurred
* Audit Departments
* We will track the number of security incidents that occurred per department to ensure compliance
* Audit users
* Audit users to test that they are putting into practice the security policies that they have been trained on
* Quarterly Vulnerability Scanning on Company Websites
* Running a vulnerability scan will allow our websites to remain on web with adequate security
* Yearly Penetration Test from Outside Firm
* Conducting a yearly penetration test from an outside firm will allow us to test the effectiveness of our security and will also allow for remediation of any security bugs that may have been found.
* Retain audit records
* Retaining the audit records in a company database allows for proper tracking and measurement of success when it comes time for the next audit.

### Contingency Planning- Policy 7

This section focuses on system restoration and implementation of alternative systems or business processes when systems are compromised or breaches. Systems will be implemented with redundancy to provide backup capabilities and for resilience against failures.

* Implement Daily Cloud Backup on ERP
* Having a daily backup of our ERP to the cloud will allow for strong resilience in the event a failure occurs
* Network Services
* All servers that provide network services such as DHCP and DNS should be designed with RAID so that in the event of a server failure the network does not go down
* Natural Disaster
* In the event of a natural disaster, we will off-load all IT services to a hot site that is ready to go for operations

### Identification and Authentication- Policy 8

The goal of this section is to enforce requirements for how users will connect to corporate services securely using encryption and ensure that their identity is valid. Any organization that may wish to connect to Blue Stripe Techs IT infrastructure will have to comply with standards outlined in this section.

* All users who may wish to connect to company resources will do so over a company provided VPN
* Having users connect to company resources over a VPN allows for a secure tunnel between the user and our IT infrastructure using encryption. This allows for safe travel of network traffic over the internet.
* MFA on User Accounts
* Enabling multi factor authentication will prove that the user is who they say they are before connecting to company resources
* WIFI
* Connecting to the company WIFI will be secured using encryption.
* A separate guest WIFI will be created for non-corporate users that will not be allowed to communicate to the company’s main network.

### Incident Response- Policy 9

This section provides an outline on what to do in the event of a breach that may occur at a system or user level.

* User Account Compromised
* In the event that a user account is compromised the user shall notify IT immediately to have their password changed.
* Malware
* If malware is found on a system IT will need to immediately shutdown the infected systems to remove the malware.
* Public Relations
* In the event of a breach notify effected users immediately and communicate to customers what went wrong and the protections we have in place

### Maintenance- Policy 10

* Inventory Database
* Any new machine before going into production should be added to the inventory database for company records to keep track of what we have
* Review Vendors
* Review current inventory every 2 years to determine if manufactures are still supporting IT software and hardware
* Update Policy
* All 400 laptop and PCs will be updated periodically through our WSUS server (Windows Server Update Services)

## Standards

### Accounts- Standard 1

All accounts will be created using [firstinitiallastname@bluestripetech.com](mailto:firstinitiallastname@bluestripetech.com). This allows for a consistent username standard for the entire company. Every account will be created using Multi factor Authentication. Every account will be configured to have no local administrative privileges to their machine to ensure no unwanted programs are installed on the machine.

### Infrastructure Standard- 2

All laptops and desktops that are put in production shall be limited to HP hardware and the windows operating system. All company offices will have access to a hard-wired connection to the internet. This will allow for greater speed and maximum use of IT infrastructure.

### Support Standard- 3

All users should submit any IT related questions to the company helpdesk. In doing so it will allow for central management of IT related requests and will make efficient use of the IT departments time as well as the users. Employees in the IT department should not proceed with major changes from word to mouth. Ensure to remind the user to submit a ticket to the help desk. Wait for manager approval to proceed with the task.

## User Domain

Policies that apply to this domain are Identification and Authentication, Termination policy, as well as the training policy.

### Controls for User Domain

* Control 1 – I recommend having user accounts configured with multi factor authentication to ensure confidentiality and integrity.
* Control 2 – Having users use the ticketing system will ensure that their requests are centrally managed
* Control 3 – Users will use a VPN client to connect to the corporate network using encryption.
* Control 4- All Users will go through a yearly security training to ensure they are up to date with company policies
* Control 5- All users will undergo a background check to ensure they meet company and legal requirements. This will allow honest individuals on the team who will have access to sensitive information

## Workstation Domain

Policies that effect the Workstation domain can fall under the maintenance policy, and configuration management

### Controls for Workstation Domain

* Control 1- An SIEM will allow for constant monitoring of workstation to detect any possible threats that may occur
* Control 2- All devices are being patched periodically with the latest drivers and firmware to ensure security and operability
* Control 3- We are applying the principle of least functoriality on workstation as they do not to have unnecessary services that may affect the security posture of our organization in an unknown way.
* Control 4- Logging has been enabled to ensure tracking of unauthorized access that may occur.

## LAN Domain

The LAN domain must be controlled in order to manage the traffic that occurs on the network. Polices that apply to this section fall under Identification and Authentication as well as Configuration management.

### Controls for LAN Domain

* Control 1- Having a Firewall in place will ensure that our organization can manage traffic within the internal network
* Control 2- Having a hard-wired connection allows for efficient use of the company’s internal resources
* Control 3- WIFI communicated is secured using encryption
* Control 4- Protection of network services from going down using redundancy

## LAN to WAN Domain

All outbound traffic is going through the firewall. Polices that apply here are Identification and Authentication as well as configuration management.

### Controls for LAN to WAN Domain

* Control 1- All communications is monitored using the company firewall
* Control 2- All ports except 67 and 68 are allowed to communicate from the LAN to WAN
* Control 3- All email going out from the organization is being kept tracking of using Mimecast

# Part 3 – Infrastructure Research B

## WAN Domain

All WAN interfaces must be protected in order to safeguard communications and have a robust network security in place that will mitigate threats from individuals who wish to cause harm to our organization. A properly configured firewall will be needed to protect our WAN. The policy that we will apply here is the configuration management policy.

### Controls for WAN Domain

* Control 1- Block all unneeded incoming connections on the WAN
* Control 2- Deploy an AV on the firewall at the perimeter that will check traffic against known threats
* Control 3- Enable a IPS on the WAN to stop malicious traffic from coming into the network

## Remote Access Domain

Identification and Authentication is the policy that will apply to this section. Anytime company resources need to be accessed over the public internet then we must make sure this communication is secure. Data flowing on the internet is susceptible to attacks. To secure our communications we will implement a range of controls based off of our Identification and Authentication policy.

### Controls for Remote Access Domain

* Control 1- All communications will be over our company provided VPN
* Control 2- All logins must be verified using MFA
* Control 3- When connecting remotely after 5 bad login attempts your account will be locked out.

## Systems/Applications Domain

This is where we offer our systems so that users can work on them. When hosting systems and services we want to make sure that they are secure. This will result in unwanted changes to our Confidentiality, integrity, and Availability. The polices that will apply here are Incident Response, Identification and Authentication, Audit and Accountability, Configuration Management, and Contingency Planning

### Controls for Systems/Applications Domain

* Control 1 – Have an active backup running. With critical systems if wrong data gets entered or something gets corrupted then it is important that we have a backup that we can revert to.
* Control 2- Deploy Anti-Virus on the system to check for malicious code that may get on the machine
* Control 3- Implement logging to properly track the system for your audit and accountability records.

# Part 4 – Conclusions and Outcomes of Overall Report

Researching polices to implement within an organization has been quite the journey. It is important to understand the business you are working for and its technology stack before we can even begin to create a policy framework. Once one understands the business they can start to draft policy to protect the business from all possible attacks or failures in processes or technology. Creating a policy is just half the battle. We then must find away to implement these policies through properly deploying controls.

# References

1- Healthcare Group, L. (n.d.). Lister Healthcare Group. Retrieved April 6, 2022, from https://listerhealthcaregroup.com/compliance/4-3-h-hipaaprivacy-privacy-response-response-and-reporting-policy/

Johnson, R., & Easttom, C. (2022). *Security policies and implementation issues*. Jones & Bartlett Learning.

2- *Final public draft NIST SP 800-53 rev. 5, security and ...* (n.d.). Retrieved April 11, 2022, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf

3- *Enterprise Service Management Framework Edition III*. Enterprise Service Management Framework. (n.d.). Retrieved April 11, 2022, from https://dodcio.defense.gov/Portals/0/Documents/DESMF%20EDITION%20III%20Signed%20June2016.pdf