# Security, Governance, Risk, & Compliance

## NIST Cybersecurity Framework Alignment
Global

## Vendor Compliance Program (VCP)

Document Revision: 1.1

Date: March 27, 2024

FORTNA

# Revision Table

| Revision | Date | Author | Revision Summary |
|---|---|---|---|
| 1.0 | 2023-01-18 | Thomas Jones | Initial submission. |
| 1.1 | 2024-03-27 | Thomas Jones | Aesthetic changes. |
| | | | |
| | | | |

# Table of Contents

# 1 Vendor Compliance Program Overview

## 1.1 Vendor Compliance Policy

Vendors must protect the confidentiality, integrity, and availability of FORTNA Group Holdings, Inc. (FORTNA) data and systems, regardless of how the data is created, distributed or stored. Vendors' security controls must be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

Management Intent: The successful implementation of FORTNA's program depends on the successful implementation of each vendor's security controls.

## 1.2 Management Direction for Vendor Cybersecurity

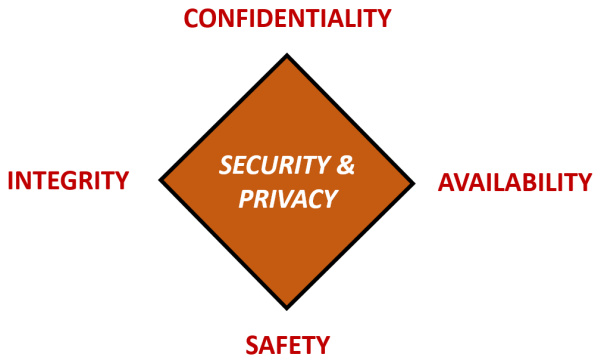
The objective of this Vendor Compliance Program (VCP) to provide direction to vendors for cybersecurity and privacy requirements that are in accordance with FORTNA's business requirements, as well as relevant laws and other legal obligations for data security and privacy. [1]

FORTNA is committed to protecting its employees, partners, clients and FORTNA from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every vendor that interacts with FORTNA data and/or systems. Therefore, it is the responsibility of VENDOR to be aware of and adhere to FORTNA's cybersecurity and privacy requirements.

Protecting FORTNA data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems, applications and services must include controls and safeguards to offset possible threats. Commensurate with risk, cybersecurity and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction.

The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:

[1] ISO/IEC 27002:2013 – 5.1




- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

## 1.3 Scope

The requirements of the VCP applies to all vendors that support FORTNA operations (e.g., suppliers, contractors, consultants, interns or other third-parties). This includes all stakeholders involved in transmitting, processing and storing FORTNA data.

## 1.4 Intent

FORTNA's **Minimum Security Requirements (MSR)** for cybersecurity are comprehensive in nature. Therefore, FORTNA expects VENDOR to also have a comprehensive set of cybersecurity and privacy policies, standards, procedures and controls to protect FORTNA's data, as well as its systems, applications and services.

VENDOR's cybersecurity program must be reasonably designed to achieve the following objectives:

- Ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of FORTNA systems, applications, services and data;
- Perform ongoing risk management practices to maintain situational awareness of risk; and
- Reasonably protect against any anticipated threats or hazards.

## 1.5 Cybersecurity Practices Alignment

The National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF) represents industry-accepted best practices for cybersecurity. Therefore, FORTNA's minimum security requirements for its vendors are consistent with NIST CSF requirements to ensure due care and due diligence in maintaining a cybersecurity management program.

# 2 Vendor's Cybersecurity Responsibilities

FORTNA expects VENDOR to maintain controls that support the National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF). The NIST CSF represents an industry-recognized set of **Minimum Security Requirements (MSR)** for cybersecurity to ensure VENDOR's due care and due diligence in maintaining its cybersecurity program.


*Figure 2: NIST Cybersecurity Framework Categories*

The NIST CSF is broken up into five (5) NIST CSF-based categories of controls that include: [2]

- Identify
- Protect
- Detect
- Respond
- Recover

## 2.1 Identify (ID)

These controls are foundational for effective cybersecurity. Understanding the business context, resources that support critical functions and the related cybersecurity risks VENDOR to focus its efforts and resources to properly secure its network.

Controls in this category focus on helping VENDOR understand the following:

- Business context;
- Resources that support critical functions; and
- Related cybersecurity risks.

### 2.1.1 Asset & Resource Management (AM)

The Asset Management (ID.AM) section of NIST CSF addresses the data, personnel, devices, systems and facilities that enable an organization to achieve business purposes that are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

[2] NIST SP 800-64 rev2 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf

#### 2.1.1.1 Hardware Management

VENDOR maintains accurate inventories of its information systems and components.[3]

#### 2.1.1.2 Software Management

VENDOR maintains accurate inventories of its approved operating systems and applications.[4]

#### 2.1.1.3 Data Flow Management

VENDOR documents its data flows (e.g., ports, protocols and services) through network diagrams and/or Data Flow Diagrams (DFDs).[5]

#### 2.1.1.4 External Information Systems

VENDOR identifies and documents information systems and services hosted or maintained by 3rd parties.[6]

#### 2.1.1.5 Resource Value Categorization

VENDOR assigns assets and resources a classification based on the business value and criticality in accordance with VENDOR's policies and standards.[7]

#### 2.1.1.6 Cybersecurity Roles & Responsibilities

VENDOR establishes and documents cybersecurity-related roles and responsibilities for the entire workforce, including third-party stakeholders (e.g., suppliers, partners, service providers, etc.).[8]

### 2.1.2 Business Environment (BE)

The Business Environment (ID.BE) section of NIST CSF addresses the organization's mission, objectives, stakeholders and activities. This information is used to inform cybersecurity roles, responsibilities and prioritize risk management decisions.

[3] ID.AM-1
[4] ID.AM-2
[5] ID.AM-3
[6] ID.AM-4
[7] ID.AM-5
[8] ID.AM-6

#### 2.1.2.1 Supply Chain Stakeholders & Interdependencies

VENDOR identifies and documents its role within the supply chain (e.g., business partners, customers) to determine interdependencies and other points of concern that may impact the supply chain.[9]

#### 2.1.2.2 Business Role Within Industry

VENDOR identifies and documents its role within its industry in an effort to identify applicable industry sector-based risk.[10]

#### 2.1.2.3 Mission & Objectives

VENDOR establishes and communicates its mission and objectives to ensure organizational awareness of its critical business functions and how that impacts VENDOR's clients.[11]

#### 2.1.2.4 Dependencies Analysis

- VENDOR identifies and documents dependencies and critical functions within its business processes that impact the delivery of critical services.[12]
-

#### 2.1.2.5 Resiliency Analysis

VENDOR identifies and documents resilience requirements to support the delivery of critical services.[13]

### 2.1.3 Governance (GV)

The Governance (ID.GV) section of NIST CSF addresses the policies, standards, procedures and processes to manage and monitor the organization's statutory, regulatory and contractual requirements. These external and internal influencers need to be understood to properly manage cybersecurity risk.

#### 2.1.3.1 Cybersecurity Policy & Standards

VENDOR documents formal cybersecurity policies, standards and procedures. This cybersecurity-related documentation is clearly made available to VENDOR's workforce.[14]

[9] ID.BE-1
[10] ID.BE-2
[11] ID.BE-3
[12] ID.BE-4
[13] ID.BE-5
[14] ID.GV-1

#### 2.1.3.2 Cybersecurity Functions

VENDOR coordinates and aligns designated cybersecurity roles with internal and external stakeholders to ensure all applicable cybersecurity and privacy responsibilities are properly addressed.[15]

#### 2.1.3.3 Statutory, Regulatory & Contractual Obligations

VENDOR adheres to all applicable cybersecurity and privacy-related statutory, regulatory and contractual obligations.[16]

#### 2.1.3.4 Cybersecurity & Privacy Program

VENDOR maintains a documented program to govern cybersecurity and privacy risks.[17]

### 2.1.4 Risk Assessment (RA)

The Risk Assessment (ID.RA) section of NIST CSF addresses the organization's understanding of cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals.

#### 2.1.4.1 Vulnerability Identification

VENDOR identifies, documents and remediates vulnerabilities as part of a Vulnerability Management Program (VMP).[18]

#### 2.1.4.2 Threat & Vulnerability Intelligence

As part of the VMP, VENDOR receives threat and vulnerability information from information sharing forums and sources.[19]

#### 2.1.4.3 Threat Assessments

As part of the VMP, VENDOR maintains a process to identify and assess both internal and external threats.[20]

[15] ID.GV-2
[16] ID.GV-3
[17] ID.GV-4
[18] ID.RA-1
[19] ID.RA-2
[20] ID.RA-3

#### 2.1.4.4 Business Impact Assessment (BIA)

As part of the VMP, VENDOR performs Business Impact Assessments (BIA) to assess the likelihood and impact associated with inherent and residual risk, considering all available risk sources (e.g., audit results, threat and vulnerability analysis and regulatory compliance).[21]

#### 2.1.4.5 Risk Determination

As part of the VMP, VENDOR assesses threats, vulnerabilities, likelihoods, impacts and compensating controls to determine overall risk.[22]

#### 2.1.4.6 Risk Responses

As part of the VMP, VENDOR identifies and prioritizes risk responses.[23]

### 2.1.5 Risk Management (RM)

The Risk Management Strategy (ID.RM) section of NIST CSF addresses the organization's priorities, constraints, risk tolerances and assumptions that are established and used to support operational risk decisions.

#### 2.1.5.1 Risk Management Framework (RMF)

VENDOR maintains an enterprise-wide Risk Management Program (RMP) to manage risk to an acceptable level.[24]

#### 2.1.5.2 Risk Tolerance Level

As part of the RMP, VENDOR's determines and documents the organization's risk tolerance level.[25]

#### 2.1.5.3 Risk Thresholds

As part of the RMP, VENDOR determines and documents thresholds for incident alerts.[26]

[21] ID.RA-4
[22] ID.RA-5
[23] ID.RA-6
[24] ID.RM-1
[25] ID.RM-2
[26] ID.RM-3

#### 2.1.6 Supply Chain Risk Management (SC)

The Supply Chain Risk Management (ID.SC) section of NIST CSF addresses the organization's priorities, constraints, risk tolerances and assumptions that are used to support risk decisions associated with managing supply chain risk.

##### 2.1.6.1 Supply Chain Risk Management

VENDOR's supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.[27]

##### 2.1.6.2 Supply Chain Risk Assessments

VENDOR's suppliers and third-party service providers of information systems, components, and services are identified, prioritized, and assessed using a risk assessment process that takes both cybersecurity and privacy into consideration.[28]

##### 2.1.6.3 Third-Party Contracts

VENDOR's contracts with its suppliers and third-party service providers are used to implement appropriate measures designed to meet the objectives of VENDOR's cybersecurity and privacy program.[29]

##### 2.1.6.4 Third-Party Assessments

VENDOR's suppliers and third-party service providers are routinely assessed using audits, test results, or other forms of evaluations to confirm those parties are meeting their contractual obligations.[30]

##### 2.1.6.5 Third-Party Response & Recovery Plans

VENDOR's conducts incident response and recovery planning testing with its suppliers and third-party service providers.[31]

## 2.2 Protect (PR)

These controls focus on implementing the appropriate safeguards to ensure the safe functionality of systems, applications and services. These activities are performed consistent with VENDOR's risk strategy and support the ability to limit or contain the impact of a potential cybersecurity event.

[27] ID.SC-1
[28] ID.SC-2
[29] ID.SC-3
[30] ID.SC-4
[31] ID.SC-5

Controls in this category focus on helping VENDOR understand the following:

- How user accounts are being managed;
- What the maintenance plan is to keep the system patched and secure;
- Change control processes;
- End user training & awareness; and
- Baseline configuration hardening that is in place.

### 2.2.1 Access Control (AC)

The Identity Management, Authentication and Access Control (PR.AC) section of NIST CSF addresses the access to physical and logical assets and associated facilities that are expected to limited access to authorized users, processes and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

#### 2.2.1.1 Logical Access Control

VENDOR manages logical access controls (e.g. User IDs and credentials) to ensure access is limited to authorized users and devices.[32]

#### 2.2.1.2 Physical Access Control

VENDOR implements mechanisms to limit physical access to assets and resources to authorized users.[33]

#### 2.2.1.3 Remote Access Control

VENDOR implements mechanisms to limit remote network access to authorized users and devices.[34]

#### 2.2.1.4 Least Privilege

VENDOR manages logical and physical access permissions that incorporate the principles of least privilege and separation of duties.[35]

#### 2.2.1.5 Network Segmentation

VENDOR implements network segregation and segmentation.[36]

[32] PR.AC-1
[33] PR.AC-2
[34] PR.AC-3
[35] PR.AC-4
[36] PR.AC-5

#### 2.2.1.6 Non-Repudiation

VENDOR verifies the identities of its users and implements technologies to ensure non-repudiation of user activities by binding all user accounts to specific individuals, including privileged users.[37]

#### 2.2.1.7 User Authentication

VENDOR implements technologies to authenticate its users, devices, and other assets commensurate with the risk of the transaction. VENDOR uses Multi-Factor Authentication (MFA) as needed to address statutory, regulatory or contractual obligations for enhanced user authentication.[38]

### 2.2.2 Awareness & Training (AT)

The Awareness and Training (PR.AT) section of NIST CSF addresses the organization's cybersecurity awareness education to ensure users are properly trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, standards, procedures and agreements.

#### 2.2.2.1 Awareness & Training

VENDOR maintains a cybersecurity awareness and training program to provide cybersecurity training and awareness for all users.[39]

#### 2.2.2.2 Privileged User Training

VENDOR provides its privileged users (e.g., system administrators) adequate training prepared them for their specific cybersecurity roles & responsibilities.[40]

#### 2.2.2.3 Service Provider Training

VENDOR implements processes to ensure its third-party stakeholders (e.g., suppliers, customers, partners) are aware of and understand their specific cybersecurity roles & responsibilities.[41]

#### 2.2.2.4 Management Training

VENDOR implements processes to ensure its management and executives are trained and adequately prepared for their specific cybersecurity roles & responsibilities.[42]

---

[37] PR.AC-6
[38] PR.AC-6
[39] PR.AT-1
[40] PR.AT-2
[41] PR.AT-3
[42] PR.AT-4

#### 2.2.2.5 Security Personnel Training

VENDOR implements processes to ensure its security personnel are trained and adequately prepared for their specific physical and cybersecurity roles & responsibilities.[43]

### 2.2.3 Data Security (DS)

The Data Security (PR.DS) section of NIST CSF addresses the management of information and records (data) consistent with the organization's risk strategy to protect the confidentiality, integrity, availability and safety of information systems and data.

#### 2.2.3.1 Protecting Data At Rest

VENDOR protects sensitive data at rest with appropriate cryptographic and physical security protections.[44]

#### 2.2.3.2 Protecting Data In Transit

VENDOR protects sensitive data being transmitted with appropriate cryptographic protections.[45]

#### 2.2.3.3 Removal of Assets & Data

VENDOR implements processes to manage the removal, transfer and disposal of assets and resources.[46]

#### 2.2.3.4 Availability Protections

VENDOR implements processes to ensure adequate availability capacity is maintained.[47]

#### 2.2.3.5 Data Leakage

VENDOR implements processes to protect against data leakage.[48]

#### 2.2.3.6 Software Integrity

VENDOR uses integrity checking mechanisms to verify software, firmware and information integrity.[49]

---

[43] PR.AT-5
[44] PR.DS-1
[45] PR.DS-2
[46] PR.DS-3
[47] PR.DS-4
[48] PR.DS-5
[49] PR.DS-6

#### 2.2.3.7 Separate Environments

VENDOR separates development/testing environment(s) from production environments.[50]

#### 2.2.3.8 Hardware Integrity

VENDOR implements technical and non-technical processes to verify hardware integrity to ensure hardware is not improperly modified.[51]

### 2.2.4 Information Protection Processes & Procedures (IP)

The Information Protection Processes and Procedures (PR.IP) section of NIST CSF addresses the cybersecurity policies standards, processes and procedures used to manage the protection of information systems and data.

#### 2.2.4.1 Baseline Configuration Requirements

VENDOR maintains baseline configurations for its technology assets that are based on industry-recognized secure practices (e.g., CIS Benchmarks, DISA STIGs or OEM security recommendations) and implements these baselines uniformly to ensure least functionality is enforced.[52]

#### 2.2.4.2 System Development Life Cycle (SDLC)

VENDOR operates a formal System Development Life Cycle (SDLC) process to ensure cybersecurity and privacy principles are identified and implemented by design.[53]

#### 2.2.4.3 Configuration Change Control

VENDOR operates a formal configuration change control process that considers cybersecurity and privacy implications for proposed changes.[54]

#### 2.2.4.4 Data Backup

VENDOR conducts, maintains and tests data backups in accordance with its business obligations.[55]

---

[50] PR.DS-7
[51] PR.DS-8
[52] PR.IP-1
[53] PR.IP-2
[54] PR.IP-3
[55] PR.IP-4

#### 2.2.4.5 Workplace Security

VENDOR ensures technical and physical controls are effective regardless a user's workplace.[56]

#### 2.2.4.6 Secure Disposal of Information

VENDOR ensures physical and digital assets are destroyed in a manner that prevents the disclosure information to unauthorized entities.[57]

#### 2.2.4.7 Protection Effectiveness Review

VENDOR implements processes to review and continuously-improve its protection processes.[58]

#### 2.2.4.8 Protection Effectiveness Sharing

VENDOR ensures FORTNA is made aware of the effectiveness of VENDOR's protection mechanisms.[59]

#### 2.2.4.9 Incident Response & Business Continuity Plans

VENDOR maintains documented, viable Incident Response Plans (IRP) and Business Continuity Plans (BCP).[60]

#### 2.2.4.10 Response & Recovery Plan Testing

VENDOR tests its IRP and BCP on at least an annual basis to ensure the validity of the plans.[61]

#### 2.2.4.11 Human Resources Security

VENDOR's Human Resources (HR) processes incorporate cybersecurity considerations for hiring, job transfer and employment termination activities.[62]

#### 2.2.4.12 Vulnerability Management Plan (VMP)

VENDOR maintains a formal Vulnerability Management Program (VMP) to proactively identify and remediate technical vulnerabilities in its systems, applications and services.[63]

---

[56] PR.IP-5
[57] PR.IP-6
[58] PR.IP-7
[59] PR.IP-8
[60] PR.IP-9
[61] PR.IP-10
[62] PR.IP-11
[63] PR.IP-12

### 2.2.5 Maintenance (MA)

The Maintenance (PR.MA) section of NIST CSF addresses the maintenance and repairs of systems and components that are performed consistent recommended practices.

#### 2.2.5.1 Maintenance Support

VENDOR performs timely maintenance of its systems, applications and services using secure practices.[64]

#### 2.2.5.2 Remote Maintenance

VENDOR perform remote maintenance of its and FORTNA assets and resources in an approved manner that prevents unauthorized access.[65]

### 2.2.6 Protective Technology (PT)

The Protective Technology (PR.PT) section of NIST CSF addresses the management of technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.

#### 2.2.6.1 Audit & Log Records

VENDOR ensures log files are created, protected and retained in accordance with VENDOR's policies and standards.[66]

#### 2.2.6.2 Removable Media

VENDOR restricts the use of removable media through administrative and technical measures.[67]

#### 2.2.6.3 Least Functionality Protections

VENDOR uses secure baseline configurations to enforce the principles of least functionality.[68]

[64] PR.MA-1
[65] PR.MA-2
[66] PR.PT-1
[67] PR.PT-2
[68] PR.PT-3

#### 2.2.6.4 Network Communications Protections

VENDOR implements appropriate technical solutions to protect the confidentiality and integrity network communications.[69]

#### 2.2.6.5 Availability Protections

VENDOR configures its systems to operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).[70]

## 2.3 Detect (DE)

These controls focus on situational awareness to ensure the timely identification and response to potential cybersecurity or privacy incidents. By decreasing response time, VENDOR increases its ability to limit or contain incidents with the least negative consequences.

Controls in this category focus on helping VENDOR understand the following:

- How incidents can be detected;
- What constitutes anomalous behavior; and
- How the systems are being logged & monitored.

### 2.3.1 Anomalies & Events (AE)

The Anomalies and Events (DE.AE) section of NIST CSF addresses the detection of anomalous activity and the understanding of potential event impacts.

#### 2.3.1.1 Network Traffic Baselines

VENDOR establishes baselines of network traffic and expected data flows to identify what activities that would be considered anomalous behavior.[71]

#### 2.3.1.2 Event Log Reviews

VENDOR analyzes detected events to understand the target(s) of attack and the methods used.[72]

[69] PR.PT-4
[70] PR.PT-5
[71] DE.AE-1
[72] DE.AE-2

#### 2.3.1.3 Event Correlation

VENDOR correlates events logs to improve detection and escalation by bringing together information from different sources to better understand what occurred.[73]

#### 2.3.1.4 Event Impact Assessment

VENDOR assesses events to determine appropriate response & recovery activities based on the potential impact.[74]

#### 2.3.1.5 Incident Alerting Thresholds

VENDOR establishes thresholds to manage incident alerting and escalation.[75]

### 2.3.2 Continuous Monitoring (CM)

The Security Continuous Monitoring (DE.CM) section of NIST CSF addresses the monitoring of information systems to identify cybersecurity events and verify the effectiveness of protective measures.

#### 2.3.2.1 Network Monitoring

VENDOR monitors network traffic to detect potential cybersecurity events.[76]

#### 2.3.2.2 Physical Monitoring

VENDOR monitors the physical environment to detect potential cybersecurity events.[77]

#### 2.3.2.3 Personnel Monitoring

VENDOR monitors individual user activities to detect potential cybersecurity events.[78]

#### 2.3.2.4 Malicious Code Detection Mechanisms

VENDOR deploys malicious code detection mechanisms to detect and eradicate malicious code.[79]

---

[73] DE.AE-3
[74] DE.AE-4
[75] DE.AE-5
[76] DE.CM-1
[77] DE.CM-2
[78] DE.CM-3
[79] DE.CM-4

#### 2.3.2.5 Mobile Code Detection Mechanisms

VENDOR detects the use of mobile code is detectable and takes corrective actions (e.g., blocking, quarantine, or alerting administrators) when unacceptable mobile code is detected.[80]

#### 2.3.2.6 Service Provider Monitoring

VENDOR monitors its third-party service providers to ensure their compliance with VENDOR's policies, standards, procedures and contractual obligations.[81]

#### 2.3.2.7 Periodic Checks

VENDOR performs periodic checks for unauthorized personnel, network connections, devices and software.[82]

#### 2.3.2.8 Production Vulnerability Scanning

VENDOR performs internal and external vulnerability assessment scans on a recurring basis.[83]

### 2.3.3 Detection Processes (DP)

The Detection Processes (DE.DP) section of NIST CSF addresses the maintenance and testing of detection processes and procedures to ensure awareness of anomalous events.

#### 2.3.3.1 Roles & Responsibilities for Event Detection & Response

VENDOR assigns roles and responsibilities for the detection and response to cybersecurity and privacy-related incidents.[84]

#### 2.3.3.2 Detection Procedures

VENDOR takes appropriate response actions in accordance with an Incident Response Plan (IRP).[85]

[80] DE.CM-5
[81] DE.CM-6
[82] DE.CM-7
[83] DE.CM-8
[84] DE.DP-1
[85] DE.DP-2

#### 2.3.3.3 Response Exercises

VENDOR tests its detection processes to ensure that the process is valid and applicable personnel understand their assigned roles and responsibilities.[86]

#### 2.3.3.4 Cybersecurity Event Coordination

VENDOR communicates event detection information among appropriate stakeholders.[87]

#### 2.3.3.5 Detection Process Improvement

VENDOR implements processes to continuously-improve its detection processes.[88]

## 2.4 Respond (RS)

These controls focus on the processes used to take action when a cybersecurity or privacy event is detected. These controls support VENDOR's ability to contain the impact of a potential incident.

Controls in this category focus on helping VENDOR understand the following:

- What response plans are in place;
- Roles and responsibilities for incident response;
- What the options are for mitigating risks from a cybersecurity incident.

### 2.4.1 Response Planning (RP)

The Response Planning (RS.RP) section of NIST CSF addresses the response processes and procedures that are executed and maintained to ensure response to detected cybersecurity incidents.

#### 2.4.1.1 Response Plan Execution

VENDOR uses its documented Incident Response Plan (IRP) when responding to cybersecurity and privacy-related incidents.[89]

[86] DE.DP-3
[87] DE.DP-4
[88] DE.DP-5
[89] RS.RP-1

### 2.4.2 Communications (CO)

The Communications (RS.CO) section of NIST CSF addresses response activities that are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

#### 2.4.2.1 Responder Roles & Responsibilities

VENDOR assigns roles and responsibilities for incident responders to ensure a successful response to cybersecurity and privacy-related incidents. [90]

#### 2.4.2.2 Incident Reporting

VENDOR reports cybersecurity and privacy-related incidents consistent with established reporting criteria.[91]

#### 2.4.2.3 Incident Information Sharing

VENDOR shares pertinent incident information with affected stakeholders.[92]

#### 2.4.2.4 Stakeholder Coordination

VENDOR coordinates incident response activities with stakeholders that are consistent with documented plans.[93]

#### 2.4.2.5 Situational Awareness

VENDOR voluntary shares cybersecurity and privacy-related incident information with external stakeholders to achieve broader situational awareness.[94]

### 2.4.3 Analysis (AN)

The Analysis (RS.AN) section of NIST CSF addresses the analysis that is conducted to ensure effective response and support recovery activities.

[90] RS.CO-1
[91] RS.CO-2
[92] RS.CO-3
[93] RS.CO-4
[94] RS.CO-5

#### 2.4.3.1 Alert Analysis

VENDOR investigates notifications from detection systems in a timely manner.[95]

#### 2.4.3.2 Impact Understanding

VENDOR evaluates the potential damage and scope of the incident to understand the potential impact of an incident.[96]

#### 2.4.3.3 Forensics

VENDOR utilizes proper forensic procedures for cybersecurity and privacy-related incidents that have the potential for legal action or data breach reporting.[97]

#### 2.4.3.4 Incident Classification

VENDOR classifies and documents incidents consistent with established response plans.[98]

#### 2.4.3.5 Incident Classification

VENDOR maintains processes to receive, analyze and respond to vulnerabilities disclosed from internal and external sources (e.g. internal testing, security bulletins, or security researchers).[99]

### 2.4.4 Mitigation (MI)

The Mitigation (RS.MI) section of NIST CSF addresses the activities to prevent the expansion of an event, mitigate its effects and resolve the incident.

#### 2.4.4.1 Contain Incidents

VENDOR implements mechanisms to contain the scope of cybersecurity incidents.[100]

#### 2.4.4.2 Mitigate Incidents

VENDOR implements mechanisms to mitigate the ramifications of cybersecurity incidents.[101]

---

[95] RS.AN-1
[96] RS.AN-2
[97] RS.AN-3
[98] RS.AN-4
[99] RS.AN-5
[100] RS.MI-1
[101] RS.MI-2

#### 2.4.4.3 New Vulnerability Response

VENDOR identifies, documents and mitigates newly-identified vulnerabilities in a timely manner.[102]

### 2.4.5 Improvements (IM)

The Improvements (RS.IM) section of NIST CSF addresses organizational response activities that are improved by incorporating lessons learned from current and previous detection/response activities.

#### 2.4.5.1 Incident Response Lessons Learned

VENDOR updates its Incident Response Plan (IRP) based on lessons learned.[103]

#### 2.4.5.2 Incident Response Strategy Update

VENDOR's management and cross-functional teams update its incident response strategy. (e.g. Integrated Security Incident Response Team (ISIRT), etc.).[104]

## 2.5 Recover (RC)

These controls focus on restoring capabilities or services that were impaired during an incident. These controls support VENDOR's ability to recover to "normal operations" in as short an amount of time and with as minimal disruption as possible.

Controls in this category focus on helping VENDOR understand the following:

- Plans that are in place to recover systems and data; and
- How recovery will be communicated to affected parties.

### 2.5.1 Recovery Planning (RP)

The Recovery Planning (RC.RP) section of NIST CSF addresses the recovery processes and procedures that are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

[102] RS.MI-3
[103] RS.IM-1
[104] RS.IM-2

#### 2.5.1.1 Recovery Plan

VENDOR uses its documented recovery plan when responding to cybersecurity and privacy-related incidents when recovery is necessary.[105]

### 2.5.2 Improvements (IM)

The Improvements (RC.IM) section of NIST CSF addresses the recovery planning and processes that are improved by incorporating lessons learned into future activities.

#### 2.5.2.1 Recovery Lessons Learned

VENDOR documents lessons learned from recovery operations and incorporates that knowledge into future recovery plans.[106]

#### 2.5.2.2 Recovery Strategy Update

VENDOR uses lessons learned from recovery operations to update its response strategies.[107]

### 2.5.3 Communications (CO)

The Communications (RC.CO) section of NIST CSF addresses the restoration activities that are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs and vendors).

#### 2.5.3.1 Public Affairs

VENDOR implements mechanisms to manage public affairs activities associated with recovery operations.[108]

#### 2.5.3.2 Reputation Recovery

VENDOR implements mechanisms to perform reputation recovery.[109]

---

[105] RC.RP-1
[106] RC.IM-1
[107] RC.IM-2
[108] RC.CO-1
[109] RC.CO-2

#### 2.5.3.3 Recovery Activities

VENDOR communicates recovery activities to applicable stakeholders, including FORTNA.[110]

[110] RC.CO-3