

CypherWorx Data Security and Privacy Plan

Summary: The purpose of this document is to present the means and methods by which CypherWorx, Inc. will comply with the requirements of New York State Education Law, Section 2-D, with regard to security and privacy of personally identifiable information.

Specific topics addressed include:

- The nature of the services provided by CypherWorx to educational agencies contracting with us.
- The extent and types of personally identifiable information collected by CypherWorx in the process of providing those services.
- The technical measures employed to secure user data and ensure users' privacy.
- The physical measures employed to secure user data and ensure users' privacy.
- The internal measures employed to ensure the confidentiality of user data, including:
 - Personnel policy that limits access to data to only those individuals who require it for the performance of their work duties
 - Training for all personnel with regard to user data security.
- Procedures to be followed in the event of a data breach or an accidental, improper, or unauthorized disclosure of data.
- The designated Data Protection Officers responsible for the execution of and enforcement of this plan.

1. Definitions

The following definitions will apply throughout this document:

- a. **We/us/our** shall be understood to refer to CypherWorx, Inc.
- b. **Client** shall be understood to refer to the school, board of cooperative educational services, or other *educational agency* (as defined under Section 2-D) entering into a contract with CypherWorx.
- c. **Learner** shall be understood to refer to any individual making use of the services offered by CypherWorx under the provisions of a contract with a client.
- d. **Personally Identifiable Information (or PII)** shall be understood to include that which is defined as student, teacher, or principal PII under Section 2-D, as well as data of a similar nature associated with other learners such as client staff, alumni, or parents of client students.
- e. **Client contract** shall be understood to refer to the contract between CypherWorx and a client.

2. Nature of Services Provided

- a. As a *third party contractor* (as defined under Section 2-D), CypherWorx will make a broad selection of e-learning courses available for the use of learners associated with the client.

- b. These courses represent additional learning opportunities for learners and are not intended to be part of any client curriculum.
- c. These e-learning courses will be delivered via one of two methods, as specified in the client contract:
 - (1) Learners will log into CollaborNation, the Learning Management System (LMS) developed and maintained by CypherWorx.
 - (2) Learners will log into an LMS provided by the client. E-learning courses will be made available to that LMS from a CypherWorx-controlled server.
- d. Learners associated with a client fall into three categories: Students and alumni, parents, and faculty and staff.
- e. Subject to the specific provisions of the client contract, the client can make these services available to learners of their choosing from among these three groups.

3. Extent of Data Collected

- a. The personally identifiable information (PII) collected by CypherWorx is limited to what is necessary to deliver the services being provided.
- b. For learners logging into CollaborNation, we collect:
 - (1) Learner's first and last name.
 - (2) Learner's email address (which serves as their User ID when logging into CollaborNation).
- c. For learners accessing our e-learning courses via a client-provided LMS, we collect:
 - (1) Learner's name (if provided by the client's LMS).
 - (2) Learner's unique ID (as determined and provided by the client's LMS). This may be an email address, a student ID number, or some other unique identifier used by the client's system.
- d. For all learners, we collect data directly resulting from their interaction with our e-learning courses, including the following:
 - (1) Which e-learning courses the learner has chosen to engage with.
 - (2) The learner's lesson status for each of those courses, which is one of the following values: Not Attempted, Incomplete/In Progress, Failed, Completed, or Passed.
 - (3) The calendar date and time upon which a learner:
 - (a) Selected (self-assigned) a given course.
 - (b) First opened a given course.
 - (c) Last interacted with a given course.
 - (d) Failed, completed, or passed a given course.
 - (e) Received a certificate (if applicable) for successful completion of a given course.
 - (4) The total elapsed time a learner has spent interacting with a given course.
 - (5) The elapsed time of a learner's most recent interaction with a given course.
 - (6) The page or slide of a course a learner was on when they exited the course ("bookmarking"), to facilitate resuming the course where the learner left off, if applicable.
 - (7) The learner's final score (if applicable) for a given course.

- e. We **do not** collect potentially sensitive PII such as physical address, age, date of birth, sex, gender, Social Security number, health- and/or disability-related information, or any form of payment information.

4. Data Security (Technical)

- a. CypherWorx contracts with Amazon Web Services (AWS) for the hosting of our application and database servers, and makes use of the robust security features and services provided by AWS. An overview of AWS Cloud Security is available here: <https://aws.amazon.com/security/>
- b. Encryption
 - (1) All PII is encrypted both at rest and in transit.
 - (2) The encryption methods employed meet or exceed the specifications of the Payment Card Industry Data Security Standard (PCI DSS).
- c. Application and database servers are protected from unauthorized access by firewalls and intrusion-detection systems.
- d. Routine security patches and software updates are applied regularly.
- e. High priority, urgent security patches are applied as quickly as possible.
- f. Security assessments are performed regularly.

5. Data Security (Physical)

- a. As noted in the preceding section, CypherWorx contracts with Amazon Web Services (AWS) for the hosting of our application and database servers, and responsibility for physical access security rests with AWS.
- b. The physical security measures of AWS data centers are summarized here: <https://aws.amazon.com/compliance/data-center/controls/>

6. Data Security (Internal Access Restrictions)

- a. Access to learner PII among CypherWorx personnel is limited to those whose job functions require it, following “least privilege” principles. In specific:
 - (1) Programming staff: The development and maintenance of the CollaborNation LMS and associated systems requires that programmers are able to:
 - (a) View and modify the structure and content of the databases in which learner PII is housed.
 - (b) Access learner accounts for purposes of identifying, recreating, and correcting errors in the software.
 - (2) Customer Support staff: In order to perform their duties, our Customer Support personnel require the ability to access learner accounts in the CollaborNation LMS so that they can:
 - (a) Provide technical assistance to learners who are having difficulties.
 - (b) Generate reports or transcripts of learners’ e-learning activity in compliance with the client contract, the requirements of Section 2-D, and/or the Parents’ Bill of Rights.

- b. CypherWorx personnel who do not have a valid need to access learner PII to fulfill their work duties shall not be permitted access.

7. Data Security and Confidentiality Training

- a. All CypherWorx personnel have received or will receive annual training with regard to the security and confidentiality of learner PII.
- b. This training will include:
 - (1) Permissible and prohibited uses of learner PII under Section 2-D.
 - (2) Which personnel should and should not have access to learner PII.
 - (3) Required security practices for personnel who do have access to learner PII.
 - (4) Actions to be taken by personnel in the event they become aware of:
 - (a) A breach of database or application server security.
 - (b) Unauthorized access to learner PII.
 - (c) Accidental or deliberate/malicious disclosure of learner PII.
 - (d) Use of PII in a manner or for a purpose prohibited by Section 2-D.

8. Security Breach Response

- a. In the event of any breach of the security or privacy of learner PII, CypherWorx will:
 - (1) Ascertain the nature of the breach.
 - (2) Take whatever actions are necessary to end the breach.
 - (3) Determine the extent of the breach, in terms of what learner PII may have been affected.
 - (4) Report the breach and its extent to the client, so that the client can then comply with the breach notification requirements of Section 2-D.
- b. Breaches of learner PII security or privacy include the following:
 - (1) Electronic breaches of database or application server security.
 - (2) Physical breaches of database or application server security.
 - (3) Accidental disclosure of learner PII.
 - (4) Deliberate/malicious disclosure of learner PII.

9. Data Protection Officers

- a. We have designated a team of two individuals to oversee adherence to the provisions of this plan. They are:
 - (1) Dan Quackenbush, Chief of Information Technology
(dquackenbush@cypherworx.com)
 - (2) Mike Maether, Vice President of Business Development
(mmaether@cypherworx.com)

06232022 DQ

Appendix A
Compliance With New York State Education Law Section 2-d Addendum ("Addendum")

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and [COMPANY], Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Definitions

As used in this Agreement and related documents, the following terms shall have the following meanings: "Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

- (a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security
(<https://www.monroe.edu/domain/1478>)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (<https://www.monroe.edu/6320>)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

Chief Privacy Officer
New York State Education Department
Room 863 EBA
89 Washington Avenue
Albany, New York 12234.

or
Monroe One Data Protection Officer
William Gregory
Monroe #1 BOCES
41 O'Connor Road
Fairport, NY 14450

Supplemental Information About Agreement Between CypherWorx, Inc. and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide CypherWorx Inc providing training content and Learning Content Management System to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

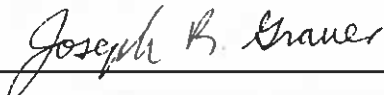
(d) The effective date of this Agreement shall be February 1, 2024 and the Agreement shall remain in effect until June 30, 2026, unless sooner by either party for any reason upon thirty (30) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vendor affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.



Vendor Signature

January 29, 2024

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Please refer to "CypherWorx Data Security and Privacy Plan" for details.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please refer to "CypherWorx Data Security and Privacy Plan" for details.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Please refer to "CypherWorx Data Security and Privacy Plan" for details.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Please refer to "CypherWorx Data Security and Privacy Plan" for details.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Please refer to "CypherWorx Data Security and Privacy Plan" for details.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Educational agencies can download and store data from the Learning Management System (LMS) at any time. In the event of service termination, CypherWorx is available to collaborate with the educational agency to facilitate the transition of data upon request.

7	Describe your secure destruction practices and how certification will be provided to the EA.	As an IACET-accredited provider, we adhere to the obligation of retaining training records for a mandatory period of seven years. Our practice refrains from proactive data destruction, recognizing the potential utility of accessing course completion records for learners. In the event that the Educational Authority (EA) expresses the intent to have data expunged upon contract termination, a written request is required. Upon receipt, we commit to collaborating with the EA to facilitate the secure and compliant destruction of the specified data.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please refer to "CypherWorx Data Security and Privacy Plan" for details.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1(A) - NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	<p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.</p>	<p>Purpose: The purpose of this Asset Management (ID.AM) Policy is to establish guidelines and procedures for identifying and managing the data, personnel, devices, systems, and facilities that enable the organization to achieve its business purposes. This policy ensures that assets are managed consistent with their relative importance to organizational objectives and the organization's risk strategy.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in the identification and management of assets within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Identification of Assets: <ul style="list-style-type: none"> • All organizational assets, including data, personnel, devices, systems, and facilities, shall be identified and categorized based on their importance to achieving business objectives. • The asset identification process shall consider the criticality of assets in supporting organizational functions and goals. 2. Asset Inventory: <ul style="list-style-type: none"> • An asset inventory shall be maintained to track and document the details of identified assets. • The asset inventory shall include information such as asset type, owner, location,

Function	Category	Contractor Response
		<p>importance to business functions, and associated risks.</p> <p>3. Classification and Prioritization:</p> <ul style="list-style-type: none"> • Assets shall be classified based on their sensitivity, criticality, and importance to organizational operations. • Prioritization of assets shall be conducted to align with their relative importance to organizational objectives and the organization's risk strategy. <p>4. Access Control and Permissions:</p> <ul style="list-style-type: none"> • Access control measures shall be implemented to restrict access to assets base on their classification and importance. • Permissions for accessing and managing assets shall be granted on a need-to-know basis and aligned with organizational roles and responsibilities. <p>5. Regular Asset Review:</p> <ul style="list-style-type: none"> • Regular reviews of the asset inventory shall be conducted to ensure its accuracy and relevance. • Asset classifications and priorities shall be updated as necessary to reflect changes in business objectives and risk strategies. <p>6. Lifecycle Management:</p> <ul style="list-style-type: none"> • The lifecycle of each asset shall be managed including acquisition, deployment, maintenance, and disposal. • Disposal of assets shall be conducted securely, following established protocols to prevent unauthorized access to sensitive information. <p>7. Integration with Risk Management:</p> <ul style="list-style-type: none"> • Asset management processes shall be integrated with the organization's risk management strategy to ensure that asset identification and management align with risk priorities. • Risks associated with assets shall be regular assessed and mitigated in accordance with organizational risk policies.
	<p>Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are</p>	<p>Purpose: The purpose of this Business Environment (ID.BE) Policy is to establish guidelines and procedures for</p>

Function	Category	Contractor Response
	<p>understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>understanding and prioritizing the organization's mission, objectives, stakeholders, and activities. This information will be used to inform cybersecurity roles, responsibilities and risk management decisions within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers who are involved in cybersecurity roles, responsibilities, and risk management within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Understanding the Organization's Mission and Objectives: <ul style="list-style-type: none"> • The organization's mission and objectives shall be clearly defined, documented, and communicated to all relevant stakeholders. • All personnel shall have a comprehensive understanding of the organization's mission and objectives. 2. Stakeholder Identification and Prioritization: <ul style="list-style-type: none"> • Stakeholders, both internal and external, shall be identified and categorized based on their importance to the organization's mission and objectives. • Prioritization of stakeholders shall guide cybersecurity decisions and resource allocation. 3. Mapping Activities to Mission and Objectives: <ul style="list-style-type: none"> • All organizational activities shall be mapped to the mission and objectives to ensure alignment with strategic goals. • Regular reviews shall be conducted to assess the relevance of activities and their impact on achieving the organization's mission. 4. Informed Cybersecurity Roles and Responsibilities: <ul style="list-style-type: none"> • Cybersecurity roles and responsibilities shall be defined based on an understanding of the organization's mission, objectives, and activities. • Individuals in cybersecurity roles shall be aware of how their responsibilities

Function	Category	Contractor Response
		<p>contribute to the achievement of organizational goals.</p> <p>5. Risk Management Informed by Business Environment:</p> <ul style="list-style-type: none"> • Risk management decisions shall be informed by a comprehensive understanding of the business environment, including the mission, objectives, stakeholders, and activities. • Cybersecurity risks shall be assessed in the context of their potential impact on organizational objectives. <p>6. Regular Business Environment Reviews:</p> <ul style="list-style-type: none"> • Regular reviews of the business environment, including changes in mission, objectives, and activities, shall be conducted. • The information gathered during reviews shall be used to update cybersecurity roles, responsibilities, and risk management strategies. <p>7. Integration with Strategic Planning:</p> <ul style="list-style-type: none"> • The business environment shall be integrated into the organization's strategic planning processes. • Cybersecurity considerations shall be embedded in strategic planning to ensure a holistic approach to achieving organizational goals.
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p>	<p>Purpose: The purpose of this Governance (ID.GV) Policy is to establish guidelines and procedures for understanding, managing, and monitoring the organization's regulatory, legal, risk, environmental, and operational requirements. This information will inform the management of cybersecurity risk within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in the governance, risk management, and cybersecurity activities within the organization.</p> <p>Policy:</p>

Function	Category	Contractor Response
		<p>1. Understanding Regulatory, Legal, and Operational Requirements:</p> <ul style="list-style-type: none"> • The organization's regulatory, legal, and operational requirements shall be clearly identified, documented, and communicated to all relevant stakeholders. • All personnel shall have a comprehensive understanding of the regulatory, legal, and operational landscape relevant to their role. <p>2. Risk Management Informed by Governance:</p> <ul style="list-style-type: none"> • Governance policies, procedures, and processes shall be integrated into the organization's risk management framework • Cybersecurity risk assessments shall consider regulatory, legal, and operational requirements to ensure compliance and effective risk mitigation. <p>3. Environmental Considerations:</p> <ul style="list-style-type: none"> • Environmental requirements, including sustainability and impact considerations, shall be integrated into governance practices. • Cybersecurity initiatives shall align with environmental policies to promote sustainable and responsible practices. <p>4. Policy and Procedure Management:</p> <ul style="list-style-type: none"> • Policies and procedures related to governance, risk, and compliance shall be regularly reviewed, updated, and communicated to all relevant personnel. • Changes to policies and procedures shall be tracked and documented to ensure transparency and accountability. <p>5. Compliance Monitoring and Reporting:</p> <ul style="list-style-type: none"> • Regular monitoring of compliance with regulatory, legal, and operational requirements shall be conducted. • Compliance reports shall be generated and communicated to management to ensure visibility and adherence to governance standards. <p>6. Risk-Informed Decision Making:</p> <ul style="list-style-type: none"> • Governance information shall be used to inform decision-making processes,

Function	Category	Contractor Response
		<p>particularly in matters related to cybersecurity risk.</p> <ul style="list-style-type: none"> Decision-makers shall consider the impact of governance requirements on cybersecurity strategies and initiatives. <p>7. Continuous Improvement:</p> <ul style="list-style-type: none"> Governance processes shall be subject to continuous improvement based on lessons learned, changes in regulatory landscape, and emerging risks. Feedback loops shall be established to capture insights and recommendations for enhancing governance practices.
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>Purpose: The purpose of this Risk Assessment (ID.RA) Policy is to establish guidelines and procedures for understanding cybersecurity risks to organizational operations, assets, and individuals. This policy ensures a systematic and comprehensive approach to risk assessment within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in risk assessment activities within the organization.</p> <p>Policy:</p> <p>1. Comprehensive Risk Identification:</p> <ul style="list-style-type: none"> The organization shall conduct a comprehensive identification of cybersecurity risks to organizational operations, assets, and individuals. Risks shall be categorized based on their potential impact on mission, functions, image, reputation, assets, and individuals. <p>2. Risk Classification and Prioritization:</p> <ul style="list-style-type: none"> Cybersecurity risks shall be classified based on their likelihood and potential impact. Prioritization of risks shall be conducted to focus mitigation efforts on high-priority and high-impact risks. <p>3. Stakeholder Involvement:</p>

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Stakeholders, including key departments and personnel, shall be actively involved in the risk assessment process. • Input from stakeholders shall be considered in the identification, classification, and prioritization of cybersecurity risks. <p>4. Risk Assessment Methodology:</p> <ul style="list-style-type: none"> • A standardized risk assessment methodology shall be adopted and consistently applied across the organization. • The methodology shall include criteria for determining likelihood, impact, and risk levels, ensuring a uniform approach to risk evaluation. <p>5. Regular Risk Assessments:</p> <ul style="list-style-type: none"> • Regular risk assessments shall be conducted at defined intervals and in response to significant organizational changes. • Specialized risk assessments may be conducted for specific projects, initiatives, or areas of concern. <p>6. Documentation of Risk Findings:</p> <ul style="list-style-type: none"> • Findings from risk assessments, including identified risks, their classification, and prioritization, shall be documented. • Risk documentation shall be maintained in a secure repository, accessible to authorized personnel. <p>7. Mitigation Strategies:</p> <ul style="list-style-type: none"> • Mitigation strategies shall be developed for high-priority and high-impact risks. • The organization shall allocate resources and implement measures to reduce or eliminate identified risks. <p>8. Continuous Monitoring and Review:</p> <ul style="list-style-type: none"> • Continuous monitoring of the risk landscape shall be maintained to identify emerging threats and changes in the cybersecurity environment. • Regular reviews of the risk assessment process and outcomes shall be conducted to ensure its effectiveness and relevance.
	<p>Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are</p>	<p>Purpose: The purpose of this Risk Management Strategy (ID.RM) Policy is to establish guidelines and procedures for</p>

Function	Category	Contractor Response
	<p>established and used to support operational risk decisions.</p>	<p>defining the organization's priorities, constraints, risk tolerances, and assumptions. This information will be used to support operational risk decisions, ensuring a consistent and effective approach to risk management.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in operational risk decisions and risk management within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Establishment of Organizational Priorities: <ul style="list-style-type: none"> • Organizational priorities shall be clearly defined, documented, and communicated to all relevant stakeholders. • Priorities shall consider the mission, functions, and strategic objectives of the organization. 2. Identification of Constraints: <ul style="list-style-type: none"> • Constraints that may impact operational risk decisions shall be identified and documented. • Constraints may include budgetary limitations, regulatory requirements, and resource availability. 3. Definition of Risk Tolerances: <ul style="list-style-type: none"> • Risk tolerances shall be established to guide operational risk decisions. • Tolerances shall be defined based on the organization's risk appetite and the potential impact of risks on mission, functions, and objectives. 4. Assumptions in Risk Management: <ul style="list-style-type: none"> • Assumptions underlying operational risk decisions shall be identified, documented, and regularly reviewed. • Assumptions shall be validated to ensure their accuracy and relevance to risk management strategies. 5. Alignment with Organizational Goals: <ul style="list-style-type: none"> • The risk management strategy shall align with organizational goals, mission, and strategic objectives.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Risk decisions shall be consistent with the overall direction and priorities of the organization. <p>6. Communication of Risk Strategy:</p> <ul style="list-style-type: none"> • The risk management strategy shall be communicated to all relevant personnel to ensure a common understanding of priorities, constraints, risk tolerances, and assumptions. • Communication channels shall be established to disseminate updates and changes to the risk management strategy. <p>7. Integration with Decision-Making Processes:</p> <ul style="list-style-type: none"> • Risk management considerations shall be integrated into decision-making processes across the organization. • Operational decisions shall be informed by the established risk management strategy to ensure consistency and alignment with organizational priorities. <p>8. Continuous Review and Adjustment:</p> <ul style="list-style-type: none"> • The risk management strategy shall be subject to continuous review to address changes in organizational priorities, constraints, and risk landscape. • Adjustments to the strategy shall be made as necessary to maintain its effectiveness and relevance.
	<p>Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	<p>CypherWorx focuses exclusively on cloud-based SaaS provision for online education and does not engage in supply chain risk management services, as it operates independently without the need for a supply chain.</p>
<p>PROTECT (PR)</p>	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>Policy Statement: CypherWorx Inc. recognizes the critical role of identity management, authentication, and access control in safeguarding its information assets. This policy establishes guidelines and procedures to ensure the secure and efficient management of user identities, authentication mechanisms, and access controls to protect against unauthorized access, data breaches, and information security risks.</p>

Function	Category	Contractor Response
		<p>Objective: The primary objective of this policy is to establish a framework for the effective management of user identities, authentication processes, and access controls, thereby ensuring the confidentiality, integrity, and availability of organizational information assets.</p> <p>Scope: This policy applies to all employees, contractors, third-party entities, and any system or application that accesses the organization's information assets.</p> <p>Policy Elements:</p> <ol style="list-style-type: none"> 1. User Identity Management: <ul style="list-style-type: none"> • A centralized user identity management system will be implemented to create, modify, and deactivate user accounts. • User accounts will be assigned unique identifiers and tied to individual roles and responsibilities. 2. Authentication: <ul style="list-style-type: none"> • Multi-factor authentication (MFA) will be enforced for accessing sensitive systems, applications, and data. • Password policies will be implemented, requiring strong, regularly updated passwords. 3. Access Control: <ul style="list-style-type: none"> • Access permissions will be based on the principle of least privilege, granting users the minimum access necessary to perform their job functions. • Access rights will be reviewed regularly, and changes will be made promptly when job roles or responsibilities change. 4. Role-Based Access Control (RBAC): <ul style="list-style-type: none"> • RBAC principles will be implemented to assign access permissions based on job role and responsibilities. • Access privileges will be tailored to align with the specific needs of each role. 5. User Provisioning and De-provisioning: <ul style="list-style-type: none"> • User accounts will be provisioned promptly upon approval and de-provisioned promptly upon termination or change of responsibilities.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Automated processes will be implemented to streamline user account management and reduce the risk of unauthorized access. <p>6. Monitoring and Logging:</p> <ul style="list-style-type: none"> • Access to sensitive systems will be monitored, and logs will be regularly reviewed for suspicious activities. • An incident response plan will be in place to address any identified security incidents promptly. <p>7. Third-Party Access:</p> <ul style="list-style-type: none"> • Third-party entities accessing organization's systems or data will be subject to the same identity management, authentication, and access control standards as internal users. • Contracts with third parties will include provisions for adherence to these security standards. <p>Roles and Responsibilities:</p> <ul style="list-style-type: none"> • The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and enforcement of this policy. • System administrators and IT personnel are responsible for implementing and maintaining identity management, authentication, and access control measures. • Human Resources is responsible for timely communication of employee status changes to IT for user account management.
	<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>Policy Statement: CypherWorx Inc. recognizes the pivotal role of awareness and training in maintaining a secure and vigilant workforce. This policy establishes guidelines and procedures for creating and sustaining a comprehensive awareness and training program to enhance the understanding of information security risks and best practices among employees, contractors, and other relevant stakeholders.</p> <p>Objective: The primary objective of this policy is to promote a culture of security awareness and continuous learning within the organization, reducing the risk of</p>

Function	Category	Contractor Response
		<p>security incidents and enhancing the overall cybersecurity posture.</p> <p>Scope: This policy applies to all employees, contractors, third-party entities, and anyone with access to the organization's information systems and data.</p> <p>Policy Elements:</p> <ol style="list-style-type: none"> 1. Training Program Development: <ul style="list-style-type: none"> • A comprehensive information security training program will be developed and maintained to address the specific needs of different roles and responsibilities within the organization. • Training content will cover information security policies, procedures, best practices, and regulatory requirements. 2. Awareness Campaigns: <ul style="list-style-type: none"> • Regular awareness campaigns will be conducted to keep employees informed about current and emerging cybersecurity threats. • Campaigns may include newsletters, posters, emails, and other communication channels to reinforce key security messages 3. Phishing Awareness: <ul style="list-style-type: none"> • Employees will receive regular training on recognizing and avoiding phishing attempts • Simulated phishing exercises may be conducted to assess and improve the organization's resilience to social engineering attacks. 4. Role-Specific Training: <ul style="list-style-type: none"> • Training programs will be tailored to the specific roles and responsibilities of employees, ensuring that individuals are equipped with the knowledge and skills necessary for their job functions. 5. Compliance Training: <ul style="list-style-type: none"> • Employees will receive training on relevant laws, regulations, and industry standards related to information security. • Training programs will be updated to reflect changes in compliance requirements.

Function	Category	Contractor Response
		<p>6. Incident Response Training:</p> <ul style="list-style-type: none"> • Employees will be trained on the organization's incident response procedure. • Regular drills and tabletop exercises will be conducted to test and improve the effectiveness of the incident response plan. <p>7. Performance Measurement:</p> <ul style="list-style-type: none"> • The effectiveness of the awareness and training program will be measured through regular assessments, quizzes, and feedback mechanisms. • Metrics will be analyzed to identify areas for improvement and to track the organization's overall security awareness posture. <p>Roles and Responsibilities:</p> <ul style="list-style-type: none"> • The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and effectiveness of the awareness and training program. • Human Resources is responsible for coordinating and tracking employee training and awareness activities. • Managers and supervisors are responsible for encouraging and supporting their teams in participating in training programs.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Policy Statement: CypherWorx Inc. recognizes the critical importance of safeguarding its data assets to ensure confidentiality, integrity, and availability. This Data Security Policy establishes guidelines and procedures for the protection, handling, and management of sensitive and confidential data to mitigate risks associated with data breaches and unauthorized access.

Objective: The primary objective of this policy is to establish a comprehensive framework for securing data throughout its lifecycle, from creation and storage to transmission and disposal.

Scope: This policy applies to all employees, contractors, third-party entities, and any systems or applications that handle or store the organization's data.

Policy Elements:

1. Data Classification:

- All data will be classified based on sensitivity and criticality to the organization.
- Classification levels will determine the appropriate security controls and access restrictions.

2. Access Controls:

- Access to sensitive and confidential data will be restricted based on the principle of least privilege.
- Role-based access controls (RBAC) will be implemented to ensure that individuals only have access to the data necessary for their job functions.

3. Encryption:

- Data in transit and data at rest will be encrypted to protect against unauthorized access.
- Encryption protocols will align with industry standards and best practices.

4. Data Handling and Transmission:

- Protocols for the secure handling and transmission of data will be established and communicated to employees.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Secure channels, such as virtual private networks (VPNs), will be used for transmitting sensitive information. <p>5. Data Retention and Disposal:</p> <ul style="list-style-type: none"> • A data retention policy will be established to define the time frames for retaining different types of data. • Data that is no longer needed or has reached the end of its retention period will be securely disposed of in accordance with established procedures. <p>6. Data Backup and Recovery:</p> <ul style="list-style-type: none"> • Regular data backups will be conducted to ensure data availability and resilience in the event of data loss or system failure. • Backup procedures will be tested periodically to verify their effectiveness. <p>7. Monitoring and Auditing:</p> <ul style="list-style-type: none"> • Monitoring systems will be implemented to track access to sensitive data and detect any suspicious activities. • Regular audits will be conducted to assess compliance with data security policies and identify areas for improvement. <p>Roles and Responsibilities:</p> <ul style="list-style-type: none"> • The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and enforcement of this policy. • Data owners and custodians are responsible for classifying and safeguarding the data within their purview. • IT personnel are responsible for implementing technical controls to enforce data security.
	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>Policy Statement: CypherWorx Inc. recognizes the paramount importance of establishing robust information protection processes and procedures to safeguard sensitive information and ensure its confidentiality, integrity, and availability. This policy sets forth guidelines and procedures for the development, implementation, and maintenance of processes to protect information</p>

Function	Category	Contractor Response
		<p>assets from unauthorized access, disclosure, alteration, and destruction.</p> <p>Objective: The primary objective of this policy is to establish a structured framework for information protection processes and procedures that align with industry best practices, legal requirements, and organizational risk tolerance.</p> <p>Scope: This policy applies to all employees, contractors, third-party entities, and any systems or applications that handle or store the organization's information assets.</p> <p>Policy Elements:</p> <ol style="list-style-type: none"> 1. Information Classification: <ul style="list-style-type: none"> • All information assets will be classified based on their sensitivity and criticality to the organization. • Classification labels will be applied to data to determine appropriate protection measures. 2. Handling and Transmission: <ul style="list-style-type: none"> • Secure handling and transmission protocols will be established to protect information during its processing and transfer. • Encryption mechanisms will be employed for sensitive information in transit. 3. Access Controls: <ul style="list-style-type: none"> • Access to information will be controlled based on the principle of least privilege. • Role-based access controls (RBAC) will be implemented to ensure authorized access. 4. Data Loss Prevention (DLP): <ul style="list-style-type: none"> • DLP measures will be implemented to monitor, detect, and prevent unauthorized disclosure of sensitive information. • Policies and controls will be established to govern the use and sharing of sensitive data. 5. Incident Response:

Function	Category	Contractor Response
		<ul style="list-style-type: none"> ● Incident response procedures will be developed and maintained to address security incidents affecting information assets. ● A designated incident response team will be trained and ready to respond to information security incidents promptly. <p>6. Audit and Monitoring:</p> <ul style="list-style-type: none"> ● Regular audits and monitoring activities will be conducted to ensure compliance with information protection policies and procedures. ● Logs will be reviewed to identify and respond to suspicious activities. <p>7. Security Awareness and Training:</p> <ul style="list-style-type: none"> ● Employees will receive regular training on information protection policies and procedures. ● Awareness campaigns will be conducted to reinforce the importance of information security. <p>Roles and Responsibilities:</p> <ul style="list-style-type: none"> ● The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and enforcement of this policy. ● Information owners and custodians are responsible for classifying and protecting information assets within their purview. ● IT personnel are responsible for implementing technical controls to enforce information protection measures.
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>Policy Statement: CypherWorx Inc. acknowledges the critical role of maintenance and repairs in sustaining the reliability and functionality of industrial control and information system components. This policy outlines the guidelines and procedures to ensure that maintenance activities are conducted consistently, following established policies and procedures to maintain the</p>

Function	Category	Contractor Response
		<p>integrity, availability, and security of these critical systems.</p> <p>Objective: The primary objective of this policy is to establish a structured framework for the maintenance and repair of industrial control and information system components, ensuring that these activities align with organizational goals, industry best practices, and security requirements.</p> <p>Scope: This policy applies to all employees, contractors, and third-party entities involved in the maintenance and repair of industrial control and information system components within the organization.</p> <p>Policy Elements:</p> <ol style="list-style-type: none"> 1. Scheduled Maintenance: <ul style="list-style-type: none"> • Scheduled maintenance activities will be planned and communicated in advance to minimize disruptions to operations. • Maintenance schedules will consider peak operational times, and efforts will be made to conduct activities during designated maintenance windows. 2. Documentation and Procedures: <ul style="list-style-type: none"> • Comprehensive documentation of maintenance procedures, including step-by-step instructions and safety protocols, will be maintained. • Maintenance personnel will be trained on and adhere to documented procedures to ensure consistency and adherence to best practices. 3. Change Management: <ul style="list-style-type: none"> • All changes to industrial control and information system components, including maintenance and repairs, will follow a formalized change management process. • Changes will be reviewed, tested, and approved before implementation to prevent unintended consequences.

Function	Category	Contractor Response
		<p>4. Security Considerations:</p> <ul style="list-style-type: none"> • Maintenance activities will be performed with due consideration for the security of industrial control and information systems • Security controls, such as access restrictions and monitoring, will be in place to prevent unauthorized access during maintenance. <p>5. Backup and Recovery:</p> <ul style="list-style-type: none"> • Before undertaking maintenance activities appropriate backups of critical data and system configurations will be performed. • Recovery procedures will be in place to restore systems to their operational state in case of unexpected issues during maintenance. <p>6. Training and Qualifications:</p> <ul style="list-style-type: none"> • Maintenance personnel will undergo regular training to stay current with the latest technologies and best practices. • Qualifications and certifications will be maintained, ensuring that personnel are adequately skilled for their assigned maintenance tasks. <p>Roles and Responsibilities:</p> <ul style="list-style-type: none"> • The Chief Information Officer (CIO) is responsible for overseeing the implementation and compliance with this policy. • Maintenance personnel are responsible for following documented procedures and reporting any deviations or issues promptly. • The IT and Operations teams are responsible for coordinating scheduled maintenance activities and ensuring minimal impact on operations.
	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>Policy Statement: The organization recognizes the critical role of protective technology in safeguarding its information assets and ensuring the confidentiality, integrity, and availability of data. This policy outlines guidelines and procedures for the implementation,</p>

Function	Category	Contractor Response
		<p>management, and continuous improvement of protective technology measures to mitigate risks and enhance the overall cybersecurity posture.</p> <p>Objective: The primary objective of this policy is to establish a comprehensive framework for the deployment and maintenance of protective technology, encompassing hardware, software, and infrastructure components, to fortify the organization's defenses against cyber threats.</p> <p>Scope: This policy applies to all employees, contractors, third-party entities, and any systems or applications that handle or store the organization's information assets.</p> <p>Policy Elements:</p> <ol style="list-style-type: none"> 1. Risk Assessment: <ul style="list-style-type: none"> • Regular risk assessments will be conducted to identify and evaluate potential threats to information assets. • Risk assessments will inform the selection and deployment of protective technology measures. 2. Antivirus and Anti-malware: <ul style="list-style-type: none"> • All endpoints and servers will have up-to-date antivirus and anti-malware software installed. • Regular scans and updates will be conducted to detect and mitigate malicious software threats. 3. Intrusion Detection and Prevention Systems (IDPS): <ul style="list-style-type: none"> • IDPS solutions will be deployed to monitor network and system activities for signs of malicious behavior. • Alerts generated by IDPS will be promptly investigated, and appropriate action will be taken. 4. Firewalls and Network Segmentation: <ul style="list-style-type: none"> • Firewalls will be implemented to control and monitor traffic between networks.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Network segmentation will be employed to isolate sensitive systems and data from unauthorized access. <p>5. Patch Management:</p> <ul style="list-style-type: none"> • A patch management process will be established to ensure timely application of security patches. • Critical patches will be prioritized, tested, and deployed promptly to mitigate vulnerabilities. <p>6. Encryption:</p> <ul style="list-style-type: none"> • Data in transit and data at rest will be encrypted using industry-standard encryption algorithms. • Encryption will be applied to protect sensitive information from unauthorized access. <p>7. Incident Response:</p> <ul style="list-style-type: none"> • An incident response plan will be in place to address security incidents related to protective technology. • The incident response team will be trained and prepared to respond promptly to security incidents. <p>Roles and Responsibilities:</p> <ul style="list-style-type: none"> • The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and enforcement of this policy. • IT personnel are responsible for the selection, deployment, and maintenance of protective technology measures. • Users are responsible for reporting any suspicious activities or security concerns promptly.
<p>DETECT (DE)</p>	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>Purpose: The purpose of this Anomalies and Events Policy is to establish guidelines and procedures for the detection and understanding of anomalous activities within our organization, ensuring a proactive approach to potential security events.</p>

Function	Category	Contractor Response
		<p>Scope: This policy applies to all employees, contractors, and third-party service providers who have access to the organization's information systems.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Detection of Anomalies: <ul style="list-style-type: none"> • Security measures shall be implemented to detect anomalous activities within the organization's information systems. • Anomaly detection tools and technologies shall be regularly updated and configured to monitor network and system activities. 2. Event Monitoring: <ul style="list-style-type: none"> • Events, including security incidents and anomalies, shall be continuously monitored to identify potential risks and threats. • The monitoring process shall include the analysis of system logs, network traffic, and other relevant data sources. 3. Incident Response: <ul style="list-style-type: none"> • Upon detection of anomalous activity, the incident response team shall be notified promptly. • An incident response plan shall be in place to address and mitigate the impact of security events. 4. Investigation and Understanding: <ul style="list-style-type: none"> • An investigation shall be conducted to understand the nature and potential impact of detected anomalies. • The incident response team shall work collaboratively to assess the scope and severity of the event. 5. Documentation: <ul style="list-style-type: none"> • All anomalies and security events shall be documented in detail, including the timeline of detection, response actions taken, and the resolution status. • Documentation shall be maintained for auditing and compliance purposes. 6. Reporting:

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • The Chief Information Security Officer (CISO) shall be notified of significant anomalies and security events promptly. • Regular reports on anomalies and events shall be provided to the appropriate stakeholders, including management and relevant security personnel.
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>Purpose: The purpose of this Security Continuous Monitoring (DE.CM) Policy is to establish a framework for the ongoing monitoring of the organization's information system and assets. Continuous monitoring aims to identify cybersecurity events promptly and validate the effectiveness of protective measures.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers who have access to the organization's information systems.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Continuous Monitoring Implementation: <ul style="list-style-type: none"> • Continuous monitoring mechanisms shall be implemented to track and assess the security status of the organization's information system and assets. • Monitoring tools and technologies shall be deployed to collect and analyze relevant security data. 2. Cybersecurity Events Detection: <ul style="list-style-type: none"> • The continuous monitoring process shall focus on the timely detection of cybersecurity events, including but not limited to unauthorized access, malware infections, and suspicious network activities. • Automated alerts and notifications shall be configured to promptly notify the appropriate personnel of identified security events. 3. Protective Measures Validation: <ul style="list-style-type: none"> • The effectiveness of existing protective measures shall be regularly assessed through continuous monitoring activities.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Security controls, configurations, and safeguards shall be reviewed and adjusted as necessary to enhance their efficacy. <p>4. Incident Response Integration:</p> <ul style="list-style-type: none"> • Continuous monitoring shall be integrated with the organization's incident response plan to facilitate a rapid and coordinated response to identified cybersecurity events. • Incident response procedures shall be regularly tested and updated based on insights gained from monitoring activities. <p>5. Data Collection and Analysis:</p> <ul style="list-style-type: none"> • Relevant security data, including logs, network traffic, and system activities, shall be collected and analyzed to identify potential threats and vulnerabilities. • Analysis results shall be used to improve security posture and inform decision-making processes. <p>6. Reporting:</p> <ul style="list-style-type: none"> • Regular reports on the findings of continuous monitoring activities shall be generated and shared with relevant stakeholders. • Significant security events and trends shall be promptly reported to the Chief Information Security Officer (CISO) and other appropriate management personnel.
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>Purpose: The purpose of this Detection Processes (DE.DP) Policy is to establish guidelines and procedures for the maintenance and testing of detection processes to ensure a heightened awareness of anomalous events within the organization's information systems.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who have access to or manage the organization's information systems.</p> <p>Policy:</p> <p>1. Maintenance of Detection Processes:</p> <ul style="list-style-type: none"> • Detection processes and procedures shall be regularly reviewed and updated to align

Function	Category	Contractor Response
		<p>with the evolving threat landscape and organizational changes.</p> <ul style="list-style-type: none"> • Documentation for detection processes shall be maintained, detailing the methodologies, tools, and criteria used for anomaly detection. <p>2. Testing and Validation:</p> <ul style="list-style-type: none"> • Regular testing of detection processes shall be conducted to validate their effectiveness in identifying anomalous events. • Testing scenarios shall simulate real-world situations and include various types of anomalies to ensure comprehensive coverage. <p>3. Awareness and Training:</p> <ul style="list-style-type: none"> • Personnel involved in detection processes shall receive regular training to stay informed about the latest threat vectors, detection techniques, and tools. • Awareness programs shall be conducted to educate all employees on the importance of reporting anomalous events promptly. <p>4. Collaboration with Incident Response:</p> <ul style="list-style-type: none"> • Detection processes shall be closely aligned with the organization's incident response plan to facilitate a seamless transition from detection to response. • Information gathered from detection activities shall be shared with the incident response team for further analysis and action. <p>5. Documentation and Record-Keeping:</p> <ul style="list-style-type: none"> • Comprehensive records shall be maintained for all detection processes, including testing results, updates, and any adjustments made. • Documentation shall be available for audit purposes and to provide insights into the organization's overall detection capabilities. <p>6. Continuous Improvement:</p> <ul style="list-style-type: none"> • Lessons learned from detection process testing and real-world incidents shall be used to continuously improve detection capabilities. • Feedback loops shall be established to gather insights from security incidents and

Function	Category	Contractor Response
		<p>apply them to enhance detection methodologies.</p> <p>7. Reporting:</p> <ul style="list-style-type: none"> Any identified anomalies or suspicious activities shall be promptly reported through established channels to the relevant security personnel. Regular reports on the effectiveness and outcomes of detection processes shall be provided to management and stakeholders.
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>Purpose: The purpose of this Response Planning (RS.RP) Policy is to establish guidelines and procedures for the execution and maintenance of response processes to ensure a swift and effective response to detected cybersecurity incidents within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who have access to or manage the organization's information systems.</p> <p>Policy:</p> <ol style="list-style-type: none"> Incident Response Plan: <ul style="list-style-type: none"> An incident response plan is established, documented, and maintained to provide a structured and coordinated approach to cybersecurity incidents. The incident response plan includes roles and responsibilities, communication protocols, and predefined response actions. Execution of Response Processes: <ul style="list-style-type: none"> Upon detection of a cybersecurity incident, the incident response team shall be activated promptly in accordance with the incident response plan. Response processes shall be executed in a timely and efficient manner to contain, eradicate, and recover from the incident. Continuous Improvement:

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Lessons learned from incident response activities shall be documented and used to improve response processes. • The incident response plan shall be reviewed and updated regularly to incorporate feedback and address emerging threats. <p>4. Communication Protocols:</p> <ul style="list-style-type: none"> • Clear communication protocols shall be established to ensure effective communication within the incident response team, with other relevant personnel, and with external parties if necessary. • Regular communication updates shall be provided to management and stakeholders during the incident response process. <p>5. Training and Drills:</p> <ul style="list-style-type: none"> • Personnel involved in incident response shall receive regular training to stay update on the latest response techniques and tools. • Tabletop exercises and simulated drills shall be conducted periodically to test the effectiveness of response processes and enhance preparedness. <p>6. Documentation and Reporting:</p> <ul style="list-style-type: none"> • Comprehensive documentation of incident response activities shall be maintained, including timelines, actions taken, and outcomes. • Incident reports shall be generated and submitted to management, the Chief Information Security Officer (CISO), and other relevant stakeholders. <p>7. Legal and Regulatory Compliance:</p> <ul style="list-style-type: none"> • Incident response processes shall be designed to comply with applicable legal and regulatory requirements. • Legal counsel shall be consulted as necessary during incident response activities to ensure compliance with legal and regulatory obligations.
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>Purpose: The purpose of this Communications (RS.CO) Policy is to establish guidelines and procedures for coordinating response activities with internal and external stakeholders.</p>

Function	Category	Contractor Response
		<p>stakeholders, including external support from law enforcement agencies, to ensure effective communication during cybersecurity incidents.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in incident response activities within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Coordination with Stakeholders: <ul style="list-style-type: none"> • Response activities shall be coordinated with internal stakeholders, including but not limited to IT teams, legal, public relations, and executive management. • External stakeholders, such as law enforcement agencies, may be engaged as necessary to support and enhance incident response efforts. 2. Communication Protocols: <ul style="list-style-type: none"> • Clear communication protocols shall be established to facilitate effective communication within the incident response team and with external stakeholders. • Regular updates on the incident's status and progress shall be provided to all relevant stakeholders, both internal and external. 3. Law Enforcement Engagement: <ul style="list-style-type: none"> • In the event of a cybersecurity incident requiring external support, law enforcement agencies may be engaged with the approval of the Chief Information Security Officer (CISO) or other designated authority. • All communication with law enforcement agencies shall be conducted in accordance with legal and regulatory requirements. 4. Confidentiality and Sensitivity: <ul style="list-style-type: none"> • Information shared with internal and external stakeholders shall be treated with the utmost confidentiality and sensitivity. • Communication regarding the incident shall be limited to individuals with a legitimate need to know, and the dissemination of information shall be controlled.

Function	Category	Contractor Response
		<p>5. Media Relations:</p> <ul style="list-style-type: none"> • A designated spokesperson or communications team shall handle external communication, including interactions with the media, to ensure a consistent and controlled message. • Media statements shall be carefully crafted to provide accurate information without compromising the organization's security posture. <p>6. Training and Awareness:</p> <ul style="list-style-type: none"> • Personnel involved in communications during incident response shall receive training on communication protocols, legal considerations, and media relations. • Awareness programs shall be conducted to educate all employees on the importance of coordinated communication during cybersecurity incidents.
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>Purpose: The purpose of this Analysis (RS.AN) Policy is to establish guidelines and procedures for conducting thorough analysis to ensure an effective response and support recovery activities during cybersecurity incidents within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers who are involved in incident response and recovery efforts.</p> <p>Policy:</p> <p>1. Thorough Incident Analysis:</p> <ul style="list-style-type: none"> • A comprehensive analysis shall be conducted for each cybersecurity incident to understand the nature, scope, and impact of the incident. • Incident analysis shall encompass the examination of system logs, network traffic, and other relevant data sources. <p>2. Root Cause Analysis:</p> <ul style="list-style-type: none"> • Root cause analysis shall be performed to identify the underlying factors that led to the cybersecurity incident.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Findings from root cause analysis shall be used to implement corrective actions to prevent similar incidents in the future. <p>3. Attribution, if Possible:</p> <ul style="list-style-type: none"> • In cases where feasible, efforts shall be made to attribute the cybersecurity incident to specific threat actors or entities. • Attribution findings, if determined, shall be reported to appropriate authorities and law enforcement agencies. <p>4. Effectiveness of Response Measures:</p> <ul style="list-style-type: none"> • The effectiveness of response measures implemented during the incident shall be assessed through analysis. • Lessons learned from the analysis shall be used to enhance and optimize future incident response strategies. <p>5. Documentation and Reporting:</p> <ul style="list-style-type: none"> • Detailed documentation of the analysis process, findings, and recommendations shall be maintained. • Incident analysis reports shall be provided to the incident response team, management, and other relevant stakeholders. <p>6. Collaboration with Recovery Efforts:</p> <ul style="list-style-type: none"> • Analysis findings shall be shared with team responsible for recovery efforts to ensure a seamless transition from analysis to recovery. • Recommendations for improving recovery processes based on analysis insights shall be communicated to the appropriate personnel. <p>7. Continuous Improvement:</p> <ul style="list-style-type: none"> • Lessons learned from incident analysis shall be systematically incorporated into the organization's incident response and recovery procedures. • Regular reviews of analysis processes shall be conducted to identify opportunities for continuous improvement.
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>Purpose: The purpose of this Mitigation (RS.MI) Policy is to establish guidelines and procedures for performing activities that prevent the expansion of cybersecurity</p>

Function	Category	Contractor Response
		<p>events, mitigate their effects, and facilitate the resolution of incidents within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers who are involved in incident response and mitigation efforts.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Proactive Mitigation Measures: <ul style="list-style-type: none"> • Proactive measures shall be implemented to prevent the expansion of cybersecurity events, including the timely application of security patches, updates, and vulnerability remediation. • Ongoing risk assessments shall be conducted to identify and address potential vulnerabilities in the organization's systems and infrastructure. 2. Containment Strategies: <ul style="list-style-type: none"> • Containment strategies shall be employed to isolate and limit the impact of cybersecurity incidents. • The incident response team shall work collaboratively to identify and implement effective containment measures. 3. Resource Allocation: <ul style="list-style-type: none"> • Adequate resources, including personnel, tools, and technologies, shall be allocated to ensure a prompt and effective mitigation response. • Resource allocation shall be based on the severity and nature of the cybersecurity incident. 4. Communication of Mitigation Measures: <ul style="list-style-type: none"> • Clear communication protocols shall be established to ensure that all relevant stakeholders are informed of mitigation measures being implemented. • Regular updates on the progress of mitigation activities shall be provided to management and other appropriate personnel. 5. Resolution Planning:

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Mitigation activities shall be conducted with an ultimate goal of resolving the incident and restoring normal operations. • Resolution plans shall be developed and maintained to guide the organization through the final stages of incident response. <p>6. Continuous Monitoring during Mitigation:</p> <ul style="list-style-type: none"> • Continuous monitoring shall be maintained throughout the mitigation process to assess the effectiveness of implemented measures. • Adjustments to mitigation strategies shall be made as necessary based on real-time monitoring and analysis. <p>7. Documentation and Reporting:</p> <ul style="list-style-type: none"> • Comprehensive documentation of mitigation activities, including strategies employed and outcomes, shall be maintained. • Mitigation reports shall be provided to the incident response team, management, and other relevant stakeholders.
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>Purpose: The purpose of this Improvements (RS.IM) Policy is to establish guidelines and procedures for continually enhancing organizational response activities by incorporating lessons learned from current and previous detection and response activities.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in incident detection and response within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Lesson Learning Framework: <ul style="list-style-type: none"> • A structured framework for capturing, documenting, and analyzing lessons learned from detection and response activities shall be established. • The framework shall include processes for identifying, recording, and disseminating insights gained during incident response. 2. Post-Incident Reviews:

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Post-incident reviews shall be conducted for all cybersecurity incidents to identify areas for improvement in detection and response • The incident response team shall participate in post-incident reviews to share insights and contribute to the improvement process <p>3. Documentation of Lessons Learned:</p> <ul style="list-style-type: none"> • Detailed documentation of lessons learned, including root cause analyses, shall be maintained for each incident. • Documentation shall include recommendations for process improvements, technology enhancements, and training needs. <p>4. Implementation of Recommendations:</p> <ul style="list-style-type: none"> • Recommendations arising from lessons learned shall be systematically reviewed, prioritized, and implemented to enhance future detection and response capabilities. • Improvement initiatives shall be assigned to responsible parties with defined timelines for implementation. <p>5. Continuous Training and Awareness:</p> <ul style="list-style-type: none"> • Personnel involved in incident detection and response shall receive ongoing training to stay current with the latest techniques, tools and best practices. • Awareness programs shall be conducted to educate all employees on the importance of contributing to the lessons learned framework. <p>6. Integration with Other Policies:</p> <ul style="list-style-type: none"> • Lessons learned from detection and response activities shall be integrated into other relevant policies, such as incident response, analysis, and mitigation policies. • The organization shall maintain a cohesive approach to continuous improvement across all cybersecurity-related policies. <p>7. Metrics and Key Performance Indicators (KPIs):</p> <ul style="list-style-type: none"> • Metrics and KPIs shall be established to measure the effectiveness of improvement initiatives over time.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> Regular reviews of metrics and KPIs shall be conducted to assess the impact of lessons learned on overall incident response capabilities.
RECOVER (RC)	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>Purpose: The purpose of this Recovery Planning (RC.RP) Policy is to establish guidelines and procedures for executing and maintaining recovery processes to ensure the swift and effective restoration of systems or assets affected by cybersecurity incidents within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers, who are involved in recovery efforts within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> Establishment of Recovery Processes: <ul style="list-style-type: none"> Recovery processes shall be defined and documented to guide the organization in restoring systems or assets affected by cybersecurity incidents. The recovery plan shall include detailed procedures, roles, and responsibilities for personnel involved in the recovery process. Timely Execution of Recovery Activities: <ul style="list-style-type: none"> Recovery activities shall be executed promptly following the identification and containment of a cybersecurity incident. The incident response team shall coordinate with relevant teams to ensure a timely and efficient restoration process. Resource Allocation for Recovery: <ul style="list-style-type: none"> Adequate resources, including personnel, equipment, and tools, shall be allocated to support the recovery efforts. Resource allocation shall be based on the severity and impact of the cybersecurity incident. Testing and Validation of Recovery Procedures: <ul style="list-style-type: none"> Recovery procedures shall be regularly tested and validated to ensure their effectiveness and efficiency.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • Testing scenarios shall simulate real-world conditions to provide a comprehensive assessment of the organization's recovery capabilities. <p>5. Communication Protocols during Recovery:</p> <ul style="list-style-type: none"> • Clear communication protocols shall be established to ensure that all relevant stakeholders are informed of recovery activities. • Regular updates on the progress of recover efforts shall be provided to management ar other appropriate personnel. <p>6. Documentation and Post-Recovery Review:</p> <ul style="list-style-type: none"> • Comprehensive documentation of recovery activities, including procedures followed and outcomes, shall be maintained. • A post-recovery review shall be conducted to assess the overall effectiveness of the recovery process and identify opportunities for improvement. <p>7. Integration with Incident Response:</p> <ul style="list-style-type: none"> • Recovery planning shall be closely integrated with the incident response plan t ensure a seamless transition from incident detection and response to the recovery phase. • Lessons learned from incident response activities shall be used to improve and refine the recovery process.
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>Purpose: The purpose of this Recovery Improvements (RC.IM) Policy is to establish guidelines and procedures fo continually enhancing recovery planning and processes b incorporating lessons learned into future activities within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers who are involved in recovery planning and processes within the organization.</p> <p>Policy:</p> <p>1. Lesson Learning Framework:</p>

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • A structured framework for capturing, documenting, and analyzing lessons learned from recovery planning and processes shall be established. • The framework shall include processes for identifying, recording, and disseminating insights gained during the recovery phase. <p>2. Post-Recovery Reviews:</p> <ul style="list-style-type: none"> • Post-recovery reviews shall be conducted for all cybersecurity incidents to identify areas for improvement in recovery planning and processes. • The recovery team shall participate in post-recovery reviews to share insights and contribute to the improvement process. <p>3. Documentation of Lessons Learned:</p> <ul style="list-style-type: none"> • Detailed documentation of lessons learned, including root cause analyses and recommendations, shall be maintained for each recovery effort. • Documentation shall include recommendations for enhancing recovery plans, procedures, and resource allocation. <p>4. Implementation of Recommendations:</p> <ul style="list-style-type: none"> • Recommendations arising from lessons learned shall be systematically reviewed, prioritized, and implemented to enhance future recovery planning and processes. • Improvement initiatives shall be assigned to responsible parties with defined timelines for implementation. <p>5. Continuous Training and Awareness:</p> <ul style="list-style-type: none"> • Personnel involved in recovery planning and processes shall receive ongoing training to stay current with the latest techniques, tools and best practices. • Awareness programs shall be conducted to educate all employees on the importance of contributing to the lessons learned framework. <p>6. Integration with Other Policies:</p> <ul style="list-style-type: none"> • Lessons learned from recovery planning and processes shall be integrated into other relevant policies, such as incident response, analysis, and mitigation policies.

Function	Category	Contractor Response
	<p>Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</p>	<ul style="list-style-type: none"> • The organization shall maintain a cohesive approach to continuous improvement across all cybersecurity-related policies. <p>7. Metrics and Key Performance Indicators (KPIs):</p> <ul style="list-style-type: none"> • Metrics and KPIs shall be established to measure the effectiveness of improvement initiatives over time. • Regular reviews of metrics and KPIs shall be conducted to assess the impact of lessons learned on overall recovery capabilities. <p>Purpose: The purpose of this Restoration Communication (RC.CO) Policy is to establish guidelines and procedures for coordinating restoration activities with internal and external parties, including coordinating centers, Internet Service Providers (ISPs), owners of attacking systems, victims, other Computer Security Incident Response Teams (CSIRTs), and vendors, to ensure effective communication during the restoration phase of cybersecurity incidents within the organization.</p> <p>Scope: This policy applies to all personnel, including employees, contractors, and third-party service providers who are involved in restoration activities within the organization.</p> <p>Policy:</p> <ol style="list-style-type: none"> 1. Coordination with Internal Stakeholders: <ul style="list-style-type: none"> • Restoration activities shall be coordinated with internal stakeholders, including but not limited to IT teams, legal, public relations, and executive management. • Clear communication channels shall be established to keep internal stakeholders informed of the progress and status of restoration efforts. 2. Communication Protocols with External Parties: <ul style="list-style-type: none"> • Clear and secure communication protocols shall be established to facilitate effective communication with external parties, including coordinating centers, ISPs, owners of attacking systems, victims, other CSIRTs, and vendors.

Function	Category	Contractor Response
		<ul style="list-style-type: none"> • All external communications shall comply with legal and regulatory requirements. <p>3. Engagement with Coordinating Centers:</p> <ul style="list-style-type: none"> • In the event of a large-scale or complex cybersecurity incident, coordination with relevant coordinating centers, industry groups, or government agencies shall be initiated. • Information sharing with coordinating centers shall be conducted in accordance with established protocols. <p>4. Collaboration with ISPs and Owners of Attacking Systems:</p> <ul style="list-style-type: none"> • Restoration efforts may involve collaboration with ISPs and owners of attacking systems to address and neutralize the threat. • Clear communication channels shall be maintained to facilitate cooperation and information sharing with ISPs and the owners of attacking systems. <p>5. Communication with Victims:</p> <ul style="list-style-type: none"> • In incidents affecting external entities or customers, clear communication shall be established with the affected parties to keep them informed of restoration activities and timelines. • Victim communication shall be conducted with empathy and transparency. <p>6. Engagement with Other CSIRTs:</p> <ul style="list-style-type: none"> • Coordination with other CSIRTs shall be established when incidents involve cross-organizational or global impacts. • Information sharing with other CSIRTs shall adhere to established protocols and confidentiality requirements. <p>7. Vendor Communication and Support:</p> <ul style="list-style-type: none"> • Communication with relevant vendors shall be initiated when restoration activities involve third-party systems or services. • Vendors shall be kept informed of the incident's impact on their products or services and may be engaged for support as needed.