INFORMATION SECURITY POLICY

I. Introduction

The Information Security Policy (ISP) establishes the expectations for safeguarding the organization's information assets. This policy aligns with the standards set by the NIST and SOC for data privacy and information security.

II. Purpose

The purpose of the ISP is to ensure the protection of information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities.

III. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other workers at the organization, including all personnel affiliated with third parties.

IV. Policy

1. **Information Security:**

As a trusted member of our organization, your understanding of our Information Security Policy is vital to ensuring the safety and integrity of our shared digital resources. Guided by the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, we have implemented an Information Security Management System (ISMS) that lays the groundwork for our digital protection efforts.

Outlined below are the core elements of our ISMS:

- **Identify:** Our first step in maintaining security involves recognizing all the digital assets that need protection. This means knowing our hardware, software, and data inside and out—what they do, who uses them, and how they might be vulnerable to threats. We encourage everyone to be mindful of the digital resources they use and understand their value.

- **Protect:** Once we've identified what needs protection, we set up safeguards. This includes everything from limiting data access to those who need it, using strong passwords, and keeping our systems updated and patched. We ask that you follow all protection protocols in place and report any potential weaknesses you may notice.

- **Detect:** Quick detection of threats is crucial. We use monitoring and detection systems to identify any unusual activity, and we count on you to report anything suspicious.

- **Respond:** If a security incident does occur, we have a response plan in place. This includes specific procedures to mitigate the incident, ensure effective communication, and get systems back up and running. In such events, it's crucial to follow the instructions of our IT team promptly.

- **Recover:** In the wake of any incident, our aim is to recover and restore any affected systems or services. We learn from these events to prevent future occurrences.

Additionally, we are committed to the Service Organization Control (SOC) reporting standards. This ensures we maintain transparency about our security efforts and keep our security controls up-to-date.

2. **Risk Management:**

The organization will employ a risk-based approach to identify and manage information security risks across all departments and functions, as outlined in NIST SP 800-37.

Risk management is a critical aspect of our Information Security Policy, ensuring the safeguarding of our organization's assets, including data and technology resources. As members of our organization, your understanding of, and adherence to, our risk management process is vital to our collective security.

Our risk management process follows the guidelines set out by NIST SP 800-37's Risk Management Framework, which involves:

- **Risk Identification:** Every member of our organization is responsible for helping identify potential risks. This could include noticing a co-worker sharing their password, spotting a suspicious email, or discovering a software vulnerability. If you see something that could pose a threat to our information security, it is crucial to report it immediately to our IT or InfoSec team.
- **Risk Assessment:** Our InfoSec team regularly assesses identified risks, taking into account their likelihood and potential impact. But remember, everyone has a role to play in risk assessment. Always consider the potential risks before sharing sensitive information, downloading an attachment, or installing new software.
- **Risk Mitigation:** Our team works to mitigate risks by implementing suitable controls and measures. This may involve changes to software, processes, or behaviors. It's crucial that everyone follows any new procedures or controls put in place to reduce risk.
- **Monitoring:** We continuously monitor our systems and processes to ensure that risk mitigations are effective and to identify new risks. If you notice any new risks or find that current controls are not working, please report it to our IT or InfoSec team immediately.

Managing risk is a shared responsibility, and every action you take can help reduce our collective risk. Be vigilant, follow all information security guidelines, and remember - if you see something, say something. Together, we can keep our organization's information safe.

3. **Access Control:**

The organization will limit information access to authorized users who require it for their role, in line with the principle of least privilege (PoLP), according to NIST SP 800-53.

A critical part of our Information Security Policy is Access Control, which involves ensuring that only authorized individuals have access to our systems and data. Everyone in our organization has a role to play in maintaining effective access controls.

Our access control policy is guided by the principle of least privilege (PoLP) and the need-to-know rule, as stipulated in NIST SP 800-53. This means:

- **Least Privilege:** Each of you will have access only to the information and systems necessary to perform your duties. Please refrain from seeking access to information or systems not related to your work. If you believe you require additional access rights, contact your supervisor or the IT department for an assessment.
- **Need to Know:** Even if you have the right privileges to access certain information, you should access it only when it's necessary for your work. Unnecessary exposure of information increases the risk of accidental or deliberate misuse.

Additionally, we employ Multi-factor Authentication (MFA) and have robust password policies:

- **MFA:** We've implemented MFA on all our systems, meaning you'll often need more than just your password to access your accounts. This could include a biometric (like a fingerprint), a physical token, or a one-time code sent to your phone. Please ensure you follow all steps required by the MFA process.
- **Password Policies:** It's essential to create strong, unique passwords and change them regularly. Don't share your passwords with anyone, and be cautious of phishing attempts to steal your credentials. If you suspect your password may have been compromised, change it immediately and inform the IT department.

Remember, access control is a critical part of our defenses against cyber threats. Misused access rights can lead to data breaches or system disruptions. Be cautious and vigilant in how you use your access rights, and immediately report any anomalies or suspicions to the IT department. Your active participation helps us maintain the integrity of our systems and data.

4. **Asset Management:**

All information assets will be identified and managed through their lifecycle, with appropriate levels of protection applied.

A crucial part of our Information Security Policy is managing how we acquire, develop, and maintain our information systems. As a member of our organization, your actions and understanding play an integral role in this.

Guided by NIST SP 800-160, our policy ensures we consider security from the outset of any system's life cycle. Here's what it involves:

- **Acquisition:** When obtaining new information systems or technology, we always prioritize secure and reputable sources. Be mindful of this when introducing any new apps, software, or hardware into our system, even for trial purposes. Always consult with the IT department before making such additions.
- **Development:** When developing or implementing new systems, we apply the concept of "secure by design". If you are involved in creating new digital solutions, ensure that you follow best

practices for secure coding, consider potential threats, and validate the security of your work through testing.

- **Maintenance:** Regular maintenance of our systems is vital for security. This includes installing updates, patches, and routinely checking system performance. If you notice your systems behaving unusually or there's an update notification, don't ignore it. Report these occurrences to the IT department.

Moreover, we perform regular System Security Assessments and Authorizations:

- **Assessments:** Our IT team conducts regular evaluations of our systems to identify potential vulnerabilities. If your role involves using specific applications, ensure you understand how to use them securely and are alert to any changes that could indicate a security issue.
- **Authorizations:** Any significant changes to our systems must be authorized by the IT department. Before making any major modifications or installing new components, seek authorization to ensure that these alterations don't inadvertently introduce security risks.

In managing our information systems, everyone's contribution is crucial. Always remember to consult the IT department before making changes, use all systems responsibly and in a manner that supports their security, and be vigilant in reporting any anomalies. Together, we can ensure the resilience and integrity of our systems.

5. **Human Resources Security:**

The organization will conduct background verification checks on all employees at the time of job acceptance, commensurate with the job role and the potential impact on information security.

6. **Incident Management:**

The organization will establish an effective incident response plan to address and manage any security breach or attack, consistent with NIST SP 800-61.

7. **Physical and Environmental Security:**

The organization will secure the physical and environmental space to prevent unauthorized access, damage, and interference to the organization's premises and information.

8. **Business Continuity Planning:**

The organization will develop and maintain a business continuity plan in line with NIST SP 800-34.

9. **Regulatory Compliance:**

The organization will abide by all relevant legal, statutory, regulatory, and contractual requirements.

10. **Third-Party Security:**

The organization will enforce, through contractual arrangements, that third parties comply with this ISP when accessing or processing organization's information.

V. Policy Compliance

1. **Compliance Measurement:**

The organization's designated InfoSec Officer will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2. **Exceptions:**

Any exception to the policy must be approved by the InfoSec Officer in advance.

3. **Non-Compliance:**

Any employee found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

VI. Related Standards, Policies, and Processes

1. NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
2. NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.
3. NIST Special Publication 800-61, Computer Security Incident Handling Guide.
4. NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems.
5. SOC 1, SOC 2, and SOC 3 Reports.