BUSINESS CONTINUITY PLAN

Code:	SO-BCP-01
Version:	1.1
Date of version:	03-05-2020
Created by:	Attila Horvath
Approved by:	Anthony Birden
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
01-18-2020	0.1	Attila Horvath	Initial version
01-25-2020	1.0	Anthony Birden	Final version
03-05-2020	1.1	Anthony Birden	Update related to COVID-19

Table of contents

1. Purpose

This policy provides guidance to assist SigningOrder.com LLC personnel in performing their respective duties and responsibilities to ensure the availability of critical services of SigningOrder.com LLC.. SigningOrder.com LLC realizes that operating disruptions can occur with or without warning, and the results may be predictable or unknown. Therefore, SigningOrder.com LLC's business operations must be resilient, and the effects of disruptions in service are minimized to maintain public trust and confidence in SigningOrder.com LLC. The Company has implemented an effective Business Continuity Plan (BCP) to establish the basis to maintain and recover business processes when operations have been disrupted unexpectedly.

2. Scope

All employees and contractors of SigningOrder.com LLC., herein referenced to as "[Company]", must comply with the terms of this policy immediately.

3. Reference documents

ISO 22301:2019 Business continuity management systems

ISO 22300:2018 Security and resilience — Vocabulary

ISO 31000:2018 Risk Management Guidelines

4. Definitions

Information system – includes all servers and clients, network infrastructure, system, and application software, data, and other computer subsystems and components that are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this policy, the term information assets are applied to information systems and other information/equipment including paper documents, cloud-based service, virtual storage, and backup solutions.

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of (i) the adverse impact or magnitude of the harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and resulting from the operation of a system.

Risk management –The program and supporting processes to manage risk to organization operations (including mission, functions, image, reputation), organization assets, individuals, other organizations, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Security – A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.

Disruption – incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives

Business Continuity Plan (BCP) – A comprehensive written plan to maintain or resume business in the event of a disruption.

Business Impact Analysis (BIA) – The process of identifying the potential impact of uncontrolled, nonspecific events on Textual business processes.

Data Redundancy – Production server performs full virtual machine replication between the production data center and secondary instance every 15 minutes

Disaster Recovery Plan – A plan that describes the process to recover from major processing interruptions.

Emergency Plan – The steps to be followed during and immediately after an emergency such as a fire, tornado, bomb threat, etc.

Encryption – The conversion of information into a code or cipher.

Gap Analysis – A comparison that identifies the difference between actual and desired outcomes.

Replication – A process that duplicates data to another location over a computer network in real-time or close to real-time.

Recovery Point Objectives – The amount of data that can be lost without severely impacting the recovery of operations.

Recovery Site – An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as "hot" sites that are fully configured centers with VPN access to our data centers and "cold" sites that are operational centers without VPN connectivity to remote data centers.

Recovery Time Objectives – The period that a process can be inoperable.

Recovery Vendors – Organizations that provide recovery sites and support services for a fee.

5. Business Continuity Planning

5.1. General

This section outlines the Business Continuity Plan Policy formalized by the CEO. SigningOrder.com LLC. is operating with virtual teams only; therefore, this policy is focusing on critical operational procedures.

The purpose of this policy is to:

- Ensure the survival of SigningOrder.com LLC through a practical and on-going business impact analysis and risk assessment program.
- Protect SigningOrder.com LLC. ’s assets and those of its customers;
- Validate SigningOrder.com LLC. ’s Business Continuity Program through effective testing, independent auditing and updating changes as necessary;
- Minimize the loss of customer and public confidence; and
- Facilitate the prompt resumption of operations.

5.2. Policy Background

SigningOrder.com LLC. ’s BCP ensures the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, pandemic, technological failures, human error, or terrorism.

The objectives of this plan are to mitigate risks from both internal and external sources:

- Avoid or minimize financial loss to SigningOrder.com LLC.;
- Continue to serve customers, partners, vendors by resuming business operations and activities;
- Mitigate the negative effects disruptions can have on SigningOrder.com LLC. ’s strategic plans, reputation, operations, liquidity, credit quality, market position; and
- Maintainability to remain in compliance with applicable laws and regulations.

SigningOrder.com LLC. ’s BCP takes into account the loss of connectivity and loss of accessibility to the SaaS-based business systems and services used by the employees. The production environment related scenarios are handled in the SigningOrder.com LLC disaster recovery plan (DRP) document.

This policy identifies the types of emergencies which may occur and the procedures to be followed based on the severity of each situation.

5.3. Identified threats to Business Continuity

Fraud, Theft or Blackmail. Since fraud, theft, or blackmail may be perpetrated more easily by insiders, SigningOrder.com LLC has implemented an effective Information Security Management framework in addition to maintaining an employee awareness training program. SigningOrder.com LLC restricts access to confidential information that may be altered or misappropriated to reduce risk exposure.

Communication network error - issues with the Internet Service Providers are the employee's home or at the work-location can cause loss of connectivity for a short or extended period.

Loss of access - issues with the devices used to access the [Company] 's business systems and business systems.

Loss of SaaS services – due to an issue at the SaaS provider side, the Company is unable to access some or all the services used for business operation.

5.4. Assumptions

The policy assumes:

- Some or all critical systems, facilities or utilities are affected during an emergency or disaster;
- Staff is available to perform critical functions defined within this policy and other contingency plans;
- Minimum personnel are available to perform the critical functions defined within this policy and other contingency plans;
- Staff can be notified, and virtual teams are operational to perform critical processing, recovery, and resumption activities;
- Subsets of this policy can be used to recover from minor interruptions;

The Company has identified the course of action in the event of a regional power failure, utility failure, and telecommunications failure.

5.5. List of critical processes, systems and personal

Critical process	System(s) required	Critical person(s) to execute the process	Alternate procedure / System
Customer contacts	Production system	Operation Manager	

5.6. Appointments and Responsibility

The Company has identified the following colleagues to be appointed to participate in the Crisis Management Process:

Crisis Management Team		
Members	**Substitutes**	**Responsibilities**

Anthony Birden	N/A	Operation Manager, Team leader
Aaron Johnson		IT operation, team member

6. Business Continuity and Recovery Procedures - SigningOrder.com LLC.

In the case when an internal or external issue is escalating and involves the Company to activate the BC plans, it is automatically done when a business continuity incident is declared by the CEO. The plan is deactivated after the incident is declared to be solved. The plan activation communication can be written and oral.

6.1. Communication plans

During the business continuity incident management, only the CEO allowed to communicate with the clients, authorities, or third-parties related to the business continuity incident.

6.2. Procedures for malicious activities

In the case when a malicious activity (fraud, theft, or blackmail) causing issues, the Company will use the incident response plan to mitigate the malicious activity and contact the appropriate law enforcement agencies. Accounts to any of the systems used or managed by the Company related to the malicious activity will be suspended as a safety measure, and activities will be investigated.

Activity	Responsible	Deadline	Outcome
Suspend accounts involved in malicious activities	CTO	ASAP	Sensitive information is inaccessible
Replace devices stolen	CTO	Within 24 hours	The employee can continue work
Create new user accounts instead of the compromised ones	CTO	Within 24 hours	The employee can continue work

6.3. Procedures for pandemic quarantine

In the case when the authorities requesting everyone to stay at home to avoid the chance of infection, SigningOrder.com LLC priority is to protect its employee's health. The Company is recommending following the instruction of the authorities, including the CDC. SigningOrder's team already working from home such an order is not a significant change to the BAU procedures. However, in the case that they need to leave their homes related to work duty (for example, in the case of an Internet error), the employees must communicate with the COO beforehand.

6.4. Procedures for Communication network error

In the case, when an employee with a critical function or involvement in a critical process is unable to communicate via the Internet or access to systems due to a network issue at work location (home office, coworking office, etc), the employee must carry out the following activities for mitigation:

Activity	Responsible	Deadline	Outcome
Switch internet connection to mobile provider 3 or 4G connection using a mobile dongle or tethering option of the mobile phone.	Employee	ASAP	The is issue mitigated, business continuity ensured
If mobile internet coverage is not available, search for a suitable location with Internet access (library, coworking space, hotel conference room, office space with short-term rent option) and start executing critical tasks from there. This is a temporary solution; costs will be reimbursed.	Employee	ASAP	*The issue is mitigated, business continuity ensured.* *Note: it is recommended to purchase or have in advance privacy screen protectors, which can be used in public areas on the laptop's screens.*
Start resolving the connectivity issue with the service provider (ISP, Telecom company, etc.).	Employee	ASAP	Restore the original working conditions for home office working

6.5. Procedures for the loss of access

In the case, if the employee is losing access to the Company's systems and services due to a technical error of the endpoint device used by the employee, or the device itself is lost or stolen, the following activities need to be carried out:

Activity	Responsible	Deadline	Outcome
Notify IT operation in the case of device loss or theft	Employee	ASAP	IT operation disable access of the employee and monitors activities for the usage of the disabled accounts as an Indicator of Compromise
Notify the authorities of the device	Employee	ASAP	The device is registered

lost or theft			as stolen/lost
Replace the unusable device	Employee	ASAP	Purchase a new device
Contact IT operation to restore accounts and ask for the new authorization codes/passwords	Employee	ASAP	Access to systems and the ability to continue work

6.6. Procedures the loss of SaaS services

The Company has identified the following SaaS services as critical services for the Company's continuous operation:

- Google Suite

In the case of when one or more of the services are not available due to an issue or issues at the service provider side, the employees must carry out the following activities:

Activity	Responsible	Deadline	Outcome
Check social media and Down Detector to verify the services issues	Employee	ASAP	Verification of services unavailability
Communicate with the CEO for the clarification of BCP activation	Employee	ASAP	BCP activation, alternate and backup service usage

7. Plan Testing & Maintenance

While efforts will be made initially to construct this DRP is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Business Continuity needs of the Company will change. As a result of these two factors, this plan will need to be tested periodically to discover errors and omissions and will need to be maintained to address them.

7.1. Maintenance

The BCP updated annually, or any time a major system update or upgrade is performed, whichever is more often. The CISO responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization to complete this task.

Maintenance of the plan include (but is not limited to) the following:

- Ensuring that all team lists are up to date
- Reviewing the plan to ensure that all of the instructions are still relevant to the organization

- Making any major changes and revisions in the plan to reflect organizational shifts, changes, and goals
- Ensuring that the plan meets any requirements specified in new laws
- Other organizational specific maintenance goals

During the Maintenance periods, any changes to the Business Continuity Teams must be accounted for. If any member of a Business Continuity Team no longer works with the Company, it is the responsibility of the CEO to appoint a new team member.

7.2. Testing

SigningOrder.com LLC. is committed to ensuring that this BCP is functional. The BCP should be tested every 12 months to ensure that it is still effective. Testing the plan carried out as follows:

Walkthroughs - Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks, or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the CISO to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities

Simulations – A BCP event is simulated so normal operations are not interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Parallel Testing - A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

Full-Interruption Testing - A full-interruption test activates the total BCP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence concerning previous DRP phases cannot be overstated.

Any gaps in the BCP that are discovered during the testing phase will be addressed by the CISO as well as any resources that he/she will require.

CYBER INCIDENT RESPONSE POLICY

Code:	SO-IRP-01
Version:	1.0
Date of version:	11-22-2019
Created by:	Attila Horvath
Approved by:	Anthony Birden
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
11-11-2019	0.1	Attila Horvath	Initial draft
11-22-2019	1.0	Anthony Birden	Final version

Table of contents

1. Purpose

The purpose of this document is to define security event monitoring procedures and incident response plans. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements.

The goal of this document is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

2. Scope

This policy applies to all employees of the company.

3. Reference documents

- NIST CSF RS
- Information Security Strategy
- NY SHIELD ACT
- CALIFORNIA CONSUMER PRIVACY ACT

4. Definitions

Information system – includes all servers and clients, network infrastructure, system, and application software, data, and other computer subsystems and components that are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, email, etc.

Information assets – in the context of this policy, the term *information assets* are applied to information systems and other information/equipment including paper documents, cloud-based service, virtual storage, and backup solutions.

Information security – The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Event – An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident – An incident is an event that, as assessed by the operation team, violates the Information Security Policy; another security policy, standard, or code of conduct; or Security Incident Response Plan threatens the confidentiality, integrity, or availability of Information Systems or Institutional Data. Incidents may establish by review of a variety of sources including, but not limited to the monitoring systems, reports from clients or client's staff or outside organizations and service degradations or outages. Discovered incidents will be declared and documented in the company incident documentation log. Complete IT service outages may also be caused by security-related

incidents, but service outage procedures will be detailed in Business Continuity and/or Disaster Recovery procedures.

Incidents will be categorized according to the potential for restricted data exposure or criticality of the resource using a High-Medium-Low designation. The initial severity rating may be adjusted during plan execution. Detected vulnerabilities are not classified as incidents. The company employs tools to scan the production environment and, depending on the severity of found vulnerabilities, may warn affected users, disconnect affected machines, or apply other mitigations.

In the absence of indications of sensitive data exposure, vulnerabilities are communicated, and the company will pursue available technology remedies to reduce that risk.

5. Incident Response Plan

5.1. Incident Detection

AWS CloudWatch and CloudTrail utilized in the production environment to provide advanced log collection, analysis, and alerting services. The IT Operation and the security analyst is regularly monitoring the events. Any suspicious activity is triaged and recorded into the JIRA ticketing system.

5.2. Incident Classification

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g., cyberstalking, racism and threats against one or more individuals)
	Child/Sexual/ Violence/	Child pornography, the glorification of violence.
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. User interaction usually is necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	

Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN,
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier such as CVE name (e.g. a buffer overflow, backdoor, cross-site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing/cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access. Also includes being part of a botnet.
	Application compromise	
	Bot	
	Unprivileged account	
Availability	Dos	By this kind of an attack, a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content	Unauthorized access to information	Besides a local abuse of data and systems, information security can be endangered by a successful account or application compromise.

Security	Unauthorized modification of information	Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking).
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of email to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright-protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world-readable printers, vulnerability apparent from the VM solution, etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	Meaning of Test	Test

5.3. Incident Response Steps

5.3.1. Containment

Because the company mainly using SaaS and PaaS solutions, incident containment might require the involvement of those providers.

After an incident declared, the operation team and the CTO will work on the containment of the incident.

- Identification of possible entry point
- Review of access logs, especially with administrative privileges
- Review of AV logs
- Search the firewall logs for brute force attacks and IP's connecting more than 100 times, not on the approved IP's list
- Review of the application logs
- AWS CloudWatch and CloudTrail review

Any other steps to contain the incident.

Organization		
Role	Task	Contact info
COO	Coordinate incident analysis, communication,	Anthony.Birden@notaryloop.com
Provider Incident response team	Support incident analysis	support@aws.com
Cybersecurity analyst (contractor)	Carry out incident and log analysis, evidence collection, forensics	Attila.horvath@cisoag.com

5.3.2. Eradication

After the incident is contained, a root cause analysis shall be carried out. With that, a detailed check for any possible infection/issues shall be carried out along with the resolution. Verification of the solution needed before the recovery process can be started.

Verification steps:

- Looking for IOC (Indicator of Compromise) in the log files created after the incident
- Verify network traffic flow and source
- If patching were involved the search for the exact vulnerabilities in the Vulnerability management solution to validate that the vulnerability can't be found on the hosts
- Review user access rights
- Validate the usefulness of the backups

5.3.3. Recovery

After the issue is eradication steps, the return to regular business can be started during this process, depending on the severity of the event a CFO can initiate a so-called "hyper care" period. During this period, the team is closely monitoring all events in the system to be able to react to any repeating attack or IOC.

At the initiation of the recovery process, the CTO, with support from the team, identifies the ETA of regular business operations. The ETA is communicated within the team as well to the clients. After validation of the remediation actions (patches, hardening, firewall rules, etc), the normal business operation can be started either by involving the BC/DR plans or using the production environment standard functionality.

5.3.4. Lessons Learned

After the regular operation is restored, it is the CTO's responsibility to create a "Lessons learned" document to find answers and record lessons.

- What changes need to be made to the security?

- How should an employee be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?
- Which controls worked effectively

The lessons learned document must be shared with the team and the management.

INFORMATION SECURITY POLICY AND SECURITY OPERATION PROCEDURES

Code:	SO-ISP-01
Version:	1.1
Date of version:	15-01-2020
Created by:	Attila Horvath
Approved by:	Anthony Birden
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
19-06-2019	0.1	Attila Horvath	Initial draft
16-07-2019	1.0	Anthony Birden	Final version
15-01-2020	1.1	Anthony Birden	Minor updates

Table of contents

1. Purpose, scope, and users

The purpose of this document is to define clear rules for the use of the information system and other information assets in SIGNING ORDER (the company). The company dedicated to providing secure and reliable services to customers; the security policy, operational, and privacy framework is created and implemented based on NIST Cyber Security Framework and other NIST publications.

Users of this document are all employees and contractors of the company.

2. Reference documents

- NIST CSF v1.1
- OWASP TOP 10
- NIST 800-30

3. Definitions

Information system – includes all servers and clients, network infrastructure, system, and application software, data, and other computer subsystems and components that are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, email, etc.

Information assets – in the context of this Policy, the term *information assets* are applied to information systems and other information/equipment, including paper documents, cloud-based service, virtual storage, and backup solutions.

Information security – The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information security risk – The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems.

Privacy information – Information that describes the privacy posture of an information system or organization.

Privacy control – The administrative, technical, and physical safeguards employed within an organization to ensure compliance with applicable privacy requirements and manage privacy risks.

4. Policy requirements

4.1. Identity (NIST CSF ID)

4.1.1. Asset Management (NIST CSF ID.AM)

Signing Order shall keep an inventory of the company's internal systems, software platforms, and applications. The company shall keep a catalog of services and information systems provided by external providers.

Signing Order shall create a diagram to document the communication and data flows.

The company should prioritize its resources (such as hardware, devices, data, time, personnel, or software) based on their classification, criticality, and business value. Signing Orders shall define and establish roles and responsibilities of cybersecurity for its entice workforce and third-party stakeholders.

NIST CSF Controls references:
ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-,5 ID.AM-6

4.1.2. Business Environment (NIST CSF ID.BE)

Signing Order shall prioritize and communicate its organizational mission, objectives, and activities. The company shall identify the dependencies and critical functions for delivering critical services. Signing Order shall identify and establish the requirements to support the delivery of its critical services during all phases of incident management.

NIST CSF Controls references:
ID.BE-3, ID.BE-4, ID.BE-5

4.1.3. Governance (NIST CSF ID.GV)

Signing Order shall create, implement, and communicate the company's cybersecurity policies and procedures. The company must define the roles and responsibilities related to cybersecurity and align the roles and responsibilities with the external partners.

Signing Order shall be aware and understand the legal and regulatory requirements related to its business, including civil liberties and privacy protection. The company's risk management and governance process must handle risks related to cybersecurity.

NIST CSF Controls references:
ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4

4.1.4. Risk Assessment (ID.RA)

Signing Order shall create and implement a risk assessment process, in which:

- Asset vulnerabilities identified and documented
- Cyber threat intelligence received from information sharing forums and sources

- Threats, both internal and external, are identified and documented
- Potential business impacts and likelihoods identified
- Threats, vulnerabilities, likelihoods, and impacts used to determine the risk
- Risk responses identified and prioritized

NIST CSF Controls references:
ID.RA-1, ID.RA -2, ID.RA -3, ID.RA -4, ID.RA-5, ID.RA-6

4.1.5. Risk Management (ID.RM)

Signing Order shall establish a risk management process; the senior management must approve the process. Signing Order shall clearly define and communicate its risk tolerance; the company shall consider best practices for defining Signing Order's risk tolerance level.

NIST CSF Controls references:
ID.RM-1, ID.RM -2, ID.RM -3

4.1.6. Supply Chain Risk Management (ID.SC)

Signing Order shall create and implement a management process to manage supply chain-related risks. The stakeholders of the company must approve of the supply-chain risk management process.

Signing Order must create and maintain a list of suppliers and third-party providers of information systems and services. The company shall prioritize the supplier and provides and execute the supply chain's risk management process on them.

The company shall ensure that contractors, suppliers, and third-party partners are implementing appropriate security controls to comply with Signing Orders requirements related to information security.

Signing Order shall regularly assess (in the form of audits, test reports, questioners) supplier and third-partier so ensure that they are meeting with their contractual obligations. The company shall involve relevant third-parties and supplier to Signing Order incidents response and recovery planning and testing exercises.

NIST CSF Controls references:
ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5

4.2. Protect (NIST CSF PR)

4.2.1. Identity Management, Authentication and Access Control (PR.AC)

Signing Order shall issue identities and credentials to its users and manage, verify, revoke, and audit authorized devices, users, and processes. The company shall manage the following aspects of user access:

- Physical access to assets
- Remote access
- Access permissions and authorizations, incorporating the principles of least privilege and separation of duties

- Identities are proofed and bound to credentials and asserted in interactions

Signing Order must protect the network integrity (e.g., network segregation, network segmentation). The company must ensure that users, devices, and other assets authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

NIST CSF Controls references:
PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7

4.2.2. Awareness and Training (PR.AT)

Signing Order shall establish cybersecurity and awareness training program; the program must aim to ensure the followings:

- All users are informed and trained
- Privileged users understand their roles and responsibilities
- Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
- Senior executives understand their roles and responsibilities
- Physical and cybersecurity personnel understand their roles and responsibilities

NIST CSF Controls references:
PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5,

4.2.3. Data Security (PR.DS)

Signing Order must ensure that data protected at rest and transit. The company shall create and implement a formal process to manage (remove, transfer, and disposit) information assets. Signing Order shall ensure that the system capacity correctly managed to ensure its availability.

The company shall implement controls and protection against intentional and unintentional data leakage. Signing Order shall use integrity checking mechanisms to verify software, firmware, and information integrity in its production systems. The company shall separate the production, testing, and development environments.

NIST CSF Controls references:
PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-4, PR.DS-5, PR.DS-6, PR.DS-7

4.2.4. Information Protection Processes and Procedures (PR.IP)

Signing Order shall create and maintains a security baseline configuration for its production environment. The company shall document and implement a configuration change control process. Signing Order shall create and implement a system development life cycle. The company shall create, implement, and test backups for the production environment.

Signing Order will continuously improve its protection procedures and controls. The company shall include cybersecurity practices into its human resource practices.

Signing Order will share the effectiveness of its protection technologies and controls with relevant third-parties. The company shall create and implement Incident Response, Business Continuity, and Disaster Recovery plans, the plans must be tested.

Signing Order shall create a vulnerability management plan and implement a vulnerability management procedure.

NIST CSF Controls references:
PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-6, PR.IP-7, PR.IP-8, PR.IP-8, PR.IP-10, PR.IP-11, PR.IP-12,

4.2.5. Maintenance (PR.MA)

Signing Order shall ensure that remote maintenance of the company assets is approved, logged, and performed in a manner that prevents unauthorized access

NIST CSF Controls references:
PR.MA-2

4.2.6. Protective Technology (PR.PT)

Signing Order shall define the requirements for auditing and log management according to the associated risk level. The company must create a policy for audit logging based on the identified requirements, document, and regularly review the procedure of audit log review and management.

Signing Order shall define a policy and procedure for removable media usage, and enforce the defined controls of using and restricting removable media. The company shall define and implement the hardening requirements to its system configuration process to ensure the systems only provide pméu essential capabilities for the least functionality.

Signing Order shall protect its communication and control networks. The company must implement mechanisms to ensure the production system resilience.

NIST CSF Controls references:
PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4, PR.PT-5

4.3. Detect (NIST CSF DE)

4.3.1. Anomalies and Events (DE.AE)

Signing Order shall create a network flow baseline for the network operation related to the system. The company shall create an event detection and analysis framework and procedures to ensure the detected events reviewed. The detection and analysis framework must be capable of collecting and correlating events from multiple sources. Signing Order shall determinate the impact of the events and define a threshold of events that is triggering an incident alert.

NIST CSF Controls references:
DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5

4.3.2. Security Continuous Monitoring (DE.CM)

Signing Order shall monitor the following environments and controls to detect suspicious activities and potential cybersecurity events:

- Production environment network
- Administrator activities
- External provider activity during maintenance
- Antivirus solution
- Unauthorized access, connections, devices, software within the production environment

Signing Order shall ensure that regular vulnerability scans carried out in the production environment

NIST CSF Controls references:
DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-5, CM-6, CM-7

4.3.3. Detection Process (DE.DP)

Signing Order shall define roles and responsibilities for the detection process to ensure accountability. The company's detection process shall be

- comply with all applicable requirements
- tested
- communicated
- continuously improved

NIST CSF Controls references:
DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5,

4.4. Respond (NIST CSF RS)

4.4.1. Response Planning (RS.RP)

Signing Order shall define and implement a response plan and ensure it executed during or after an incident.

NIST CSF Controls references:
RS.RP-1

4.4.2. Communications (RS.CO)

Singing Order shall create and implement an incident response plan (IRP), the plan must define the followings:

- Personnel and their roles related to incident response
- Incident reporting criteria and process
- Incident sharing criteria and process
- Coordination with stakeholders process
- Criteria of voluntary information sharing with external stakeholders

The company must ensure that established procedures followed based on the defined criteria.

NIST CSF Controls references:
RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5

4.4.3. Analysis (RS.AN)

Signing Order shall ensure that notification and alerts from the monitoring systems investigated, the possible impact of the incident is understood, that incidents categorized according to the definition of the Incident Response Plan. The company shall carry out forensic activities related to the event.

Signing Order shall create and implement a vulnerability analysis process for disclosed vulnerabilities.

NIST CSF Controls references:
RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5

4.4.4. Mitigation (RS.MI)

Signing Order shall ensure that during the incident response process incidents contained and mitigated

Signing Order must mitigate identified vulnerabilities or document risk acceptance related to the vulnerability

NIST CSF Controls references:
RS.MI-1, RS.MI-2, RS.MI-3

4.4.5. Improvements (RS.IM)

Signing Order shall ensure that lessons learned analysis carried out after the incident response process and incorporated into the incident response plan. The company shall update the response strategies and plans regularly.

NIST CSF Controls references:
RS.IM-1, RS.IM-2

4.5. Recover (NIST CSF RC)

4.5.1. Recovery Planning (RC.RP)

Signing Order.com LLC shall use (execute) the created recovery plans during or after a cybersecurity incident

NIST CSF Controls references:
RC.RP-1

4.5.2. Recovery Planning (RC.IM)

Signing Order shall ensure that lessons learned analysis carried out after a cybersecurity incident and incorporated into the recovery plans. The company shall update the recovery strategies and plans regularly.

NIST CSF Controls references:
RC.IM-1, RC.IM-2

4.5.3. Communications (RC.CO)

SigningOrder shall create and maintain communication plans to ensure that when needed, proper communication is carried out to the public. The company should make efforts to repair its reputation if it was damaged after an incident.

SigningOrder shall communicate the recovery activities to the internal and external stakeholders as well as executive and management teams.

NIST CSF Controls references:
RC.CO-1, RC.CO-2, RS.CO-3

5. Implemented controls and procedures

5.1. Identity

5.1.1. Asset Management (NIST CSF ID.AM)

Due to the nature of the company services and technical solutions, the production environment's information asset is inventoried, and the inventory is maintained in the AWS management console. Developer, test, and production environments exist only existing in the AWS cloud.

Information assets, including external services and solutions, are categorized according to their classification, criticality, and business value. All information assets must be classified into three-level: Confidential, Internal, Public.

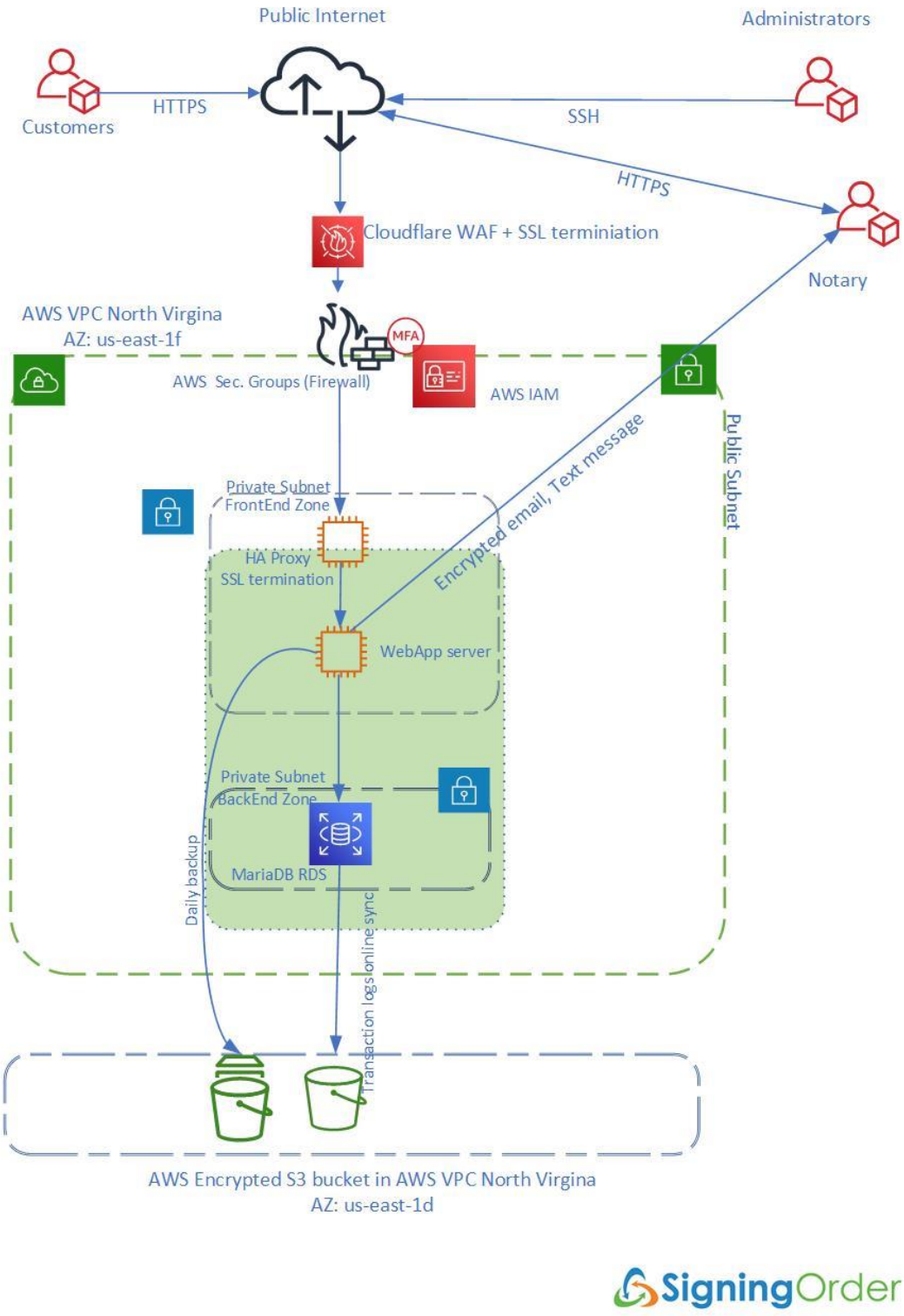
The asset register is located on the Company GDrive under /Security/Asset

All clients and user-related data are automatically classified as "Confidential" electronic, and paper-based documents shall be marked according to the classification level.

The management of information assets is the responsibility of the CEO. SigningOrder.com LLC is a company providing software as a Service. The following roles are existing to support security operations.

Task	Role
IT Operation, design, management	CTO

Mobile App and FrontEnd development	Developer
Database programming	Programmer
System operation	System Administrator
Security, vulnerability management	Information Security Officer



SigningOrder platform dataflow diagram

5.1.2. Business Environment (NIST CSF ID.BE)

The company maintains an asset register where internal and external services are identified by criticality. Any services that the SigningOrder platform is dependent on are identified and added to the incident response plan. The Business Continuity and Disaster Recovery plans are containing the minimal requirements for the company to be able to provide its services to its customers. For more details, please see the asset register: /Security/Asset and the SigningOrder BCP and DRP documents.

5.1.3. Governance (NIST CSF ID.GV)

The company information and cybersecurity are managed by the CEO, and the company is complying with the following regulations and laws: CCPA, NY Shield.

The company information security and privacy policy framework is based on the NIST CSF framework, policies, and procedures for security management and operation are created and maintained regularly.

The following documents are consisting of the policy and procedure framework of the company:

Access and Account Management Policy	SigningOrder_Access_and_Account_Management Policy_1.0.doc
Asset register	SigningOrder Asset register for ISMS.xls
Business Continuity Plan	SigningOrder_Business_Continuity_Plan__1.1.doc
Change and Patch Management	SigningOrder_Change_and_Patch_Managemt_Policy_1.0.doc
Cyber Incident Response Plan	SigningOrder_Cyber_Vulnerability_management_Policy_1.0.doc
Data Classification Policy	SigningOrder_Data_Classification_Policy_1.0.doc
Disaster Recovery Plan	SigningOrder_Disaster_Recovery_Plan_AWS_final1.doc
Encryption policy	SigningOrder_Data_Encryption_Policy_1.0.doc
Information Security Policy	SigningOrder_Information_Security_Policy_1.0.doc
Risk Management Policy	SigningOrder_Security_Risk_Management_1.0.doc
Secure Configuration and System Hardening	SigningOrder_Secure_Configuration_and_System_Hardening_Policy_1.0.doc
Security Audit and Monitoring	SigningOrder_Security_Audit_and_Monitoring_Policy_1.0.doc
Third-party Security Management Policy	Third_Party_Security_Management_Policy_1.0.doc

Software Development Life-cycle	SigningOrder_SoftwareDevelopment_Policy.doc
Vulnerability Management	SigningOrder_Cyber_Vulnerability_management_Policy_1.0.doc
Litigation Hold Policy	SigningOrder_LitigationHold_Policy.doc

Cyber and information security risks shall be managed according to the Risk Management program of SigningOrder.com LLC.

5.1.4. Risk management (NIST CSF ID.RA, ID.RM)

Technical Risk Assessment

Vulnerabilities of the production environment are continuously assessed by the AWS Inspector vulnerability solution. Threat intelligence information is provided by Amazon.

Risk Management

The company maintains a risk management framework that defines the risk assessment and management process, the risk tolerance of the company. The risk management process is maintained by the CTO.

Risk, Threats, and vulnerabilities (internal and external) are identified, assessed, and monitored continuously by the CTO in the Risk register. The company is implemented its risk assessment process based on NIST Special Publications 800-30.

For more details, please see the *SigningOrder_Security_Risk_Management_1.0.doc* document

5.2.2. 3rd party management (NIST CSF ID.SC)

The company maintains a list of 3rd party contractors; all contractors are legally obliged to protect any data related to the company. Each supplier must sign the NDA before any work that can be carried out. The company maintains the right to assess and audit it's suppliers any time during the contract period; this right is recorded in the contract.

Critical providers are obliged to provide the same level of security and availability as the company. Integration partners are obliged to provide the same level of security and availability as the company.

For more details, please see the *Third_Party_Security_Management_Policy_1.0.doc* document

5.2. Protect (NIST CSF PR)

5.2.3. Access Management (NIST CSF PR.AC)

Access to all information assets is managed. Due to the nature of the operation and the limited number of privileged users, all access control to the production and staging environment is managed only by the CTO, using an e-mail-based process. All-access rights are maintained in the relevant AWS Management Console.

Access rights are following the best practices, eg.: segregation of duty, least privilege assignment.

All user rights are reviewed yearly.

Access to supporting systems (email, JIRA, etc) are managed by the CTO based on email requests.

The production environment the network is segregated, and a firewall is separating the different network segments.

Management access is only allowed via two-factor authentications, and only accessible from approved IP addresses, any IP address which is not on the list will be rejected by the edge firewall.

Users of the information system may only access those information system assets for which they have been explicitly authorized by the asset owner.

Users may use the information system only for purposes for which they have been authorized, i.e. for which they have been granted access rights.

Users must not take part in activities that may be used to bypass information system security controls.

The privileged users are using unique usernames, password policy is configured on each server with complex password requirements, and 30 days password expiry.

Please see the *SigningOrder_Access_and_Account_Management Policy_1.0.doc* document for details.

5.2.4. Security Awareness (NIST CSF PR.AT)

All user of the company is required to take an online security awareness training session. Contractors are professional, and by signing the contract, they are acknowledging the company's security principals and their roles and duties.

5.2.5. Data Security (NIST CSF PR.DS)

Cryptographic keys (NIST CSF PR.DS-1, PR.DS-2)

SigningOrder.com LLC's cryptographic key management is based on NIST 800-57 rev. 5 part 1 recommendation.

- Symmetric cryptosystem key lengths should at least 112 bits for confidential data and 80 bits for other sensitive information identified by the company.
- Asymmetric crypto-system keys must be of a length that yields equivalent strength, (e.g., approximate equivalencies of 64 bit symmetric = 512 bit asymmetric; 80 bit = 1024 bit; 112 bit = 2048 bit; 128 bit = 3072 bit).
- All encryption mechanisms implemented to comply with this policy support a minimum of, but not limited to AES-256.

The use of proprietary encryption algorithms is not allowed for any purpose.

Data is protected with encryption when it is necessary; a minimum of 2048 bit key must use with AES 256 encryptions. Data-at-transit and data-at-rest must be protected with encryption.

The implemented access control principals are protecting against data leakage. AWS management console is providing a built-in capacity management solution; if any of the environment requires a capacity extension, it could be easily done due to the virtual environment and sophisticated cloud technology. Auto-scaling is enabled for the environments.

Due to legal and contractual obligations, the organization protects the following individual systems or information using encryption controls:

Name of system/ type of information	***Encryption tool***	***Encryption algorithm***
SigningOrder platform all data	MariaDB encryption	AES 256
AWS OS and S3 storage	AWS	AES 256

Data at transit

The service is only available via HTTPS, the communication between the frontend and the AWS RDS MariaDB database is encrypted with SSL connection. Archive, backups are also transferred and stored encrypted.

Database encryption

All data stored in the database is encrypted with AWS RDS KSM technology and protects sensitive data while the data in use during movement between clients and servers, and while the data is in rest.

Data at rest

Data at rest (archive, backup) is encrypted automatically via AWS RDS backup and archiving solution. The access to the archived data is only possible via an HTTPS interface; the data is encrypted with AES-256 encryption us Galois/Counter Mode.

Key management

Encryption keys are stored at the AWS KMS key vault solution, which is providing FIPS-140 Level 2 validated HSM for key storage. Access to the vault is limited to the CTO only.

For details, please see the *SigningOrder_Data_Encryption_Policy_1.0.doc* document.

5.2.6. Information Protection Processes and Procedures (PR.IP)

The SigningOrder's platform is running in AWS, CIS hardening guidelines based images are used for the operating systems of the EC2 instances (CentOS). AWS Inspector is continuously monitoring the environment compliance with the implemented guidelines.

For details, please see:

the *SigningOrder_Secure_Configuration_and_System_Hardening_Policy_1.0.doc* document.

Changes are managed according to the change management policy; all change is tracked in the ticketing system.

For details, please see the *SigningOrder_Change_and_Patch_Managemt_Policy_1.0.doc* document.

The company has created BCP, DRP, and IRP plans for details, please see the following documents:

SigningOrder_Business_Continuity_Plan__1.1.doc

SigningOrder_Cyber_Vulnerability_management_Policy_1.0.doc

SigningOrder_Disaster_Recovery_Plan_AWS_final1.doc

The plans are tested and updated annually.

Developer, Test, and Production environments are separated, and changes are managed in a controlled way. The development code is stored in GitHub (access only allowed via HTTPS and using two-factor authentication). Changes and the development process are managed in the Asana ticketing system. All steps are documented and recorded in the ticketing system.

Any new development or changes first deployed into the developer environment, via the standard Github, deploy method, and after testing and peer review deployed into the test environment for boarder testing, including UAT and regression testing. After the testing results are accepted by the CTO, approval to deployment into the production environment is given. In the case that the change is affecting the customers, the company issues a notification statement according to its approved communication plan.

SigningOrder's platform is continuously assessed by AWS inspector for vulnerabilities.

Configuration changes are managed in the Jira ticketing system as well.

The database's transaction log that is continuously synced to encrypted S3 storage. The business logic and running environment are backed up daily with full image snapshots taken and stored securely with AWS backup to store in a separate availability zone in an encrypted S3 bucket. A full backup is also made before significant changes and releases.

The integrity test of the backups is checked out every12 months manually by the operation team.

The company's Recovery Time Objective is 24 hours in the case of the loss of both Availability Zones, where the solution is operating. Recovery Point Objective is 0 min and ensured with the continuous sync backup of the database transaction logs. In the case of an incident is escalated, and a business continuity plan is initiated, the operation team can access the environment from several whitelisted IP addresses that are geographically distributed.

Due to the nature of the business space where the company is operating a strict security screening and vetting process is in place managed by the HR department.

Patches are automatically deployed in the development environment for initial testing and assessment; after 2 days of testing, the patches are deployed in the test and production environment—the scheduling and distribution of the patches done via AWS Patching solution.

The company is using AWS Inspector as a vulnerability management solution. Internal vulnerability scans are done weekly, reports are analyzed, and if necessary, a ticket is created to manage the vulnerability. Vulnerabilities are rated based on severity between 1-5, where 5 is the highest severity. Level 5 severity categorized vulnerabilities must be resolved within 3 working days.

External vulnerability scanning is done monthly by Qualys external scanners.

The company is ordering an external black box penetration testing annually, each year using a different vendor.

After performing an assessment, AWS Inspector produces a detailed list of security findings that are organized by level of severity. This automated technology can adhere to other established processes for change control, ticketing, and asset security. The results of the assessment can be reviewed in the AWS Security HUB.

Upon receipt of the reports, the Operations Team is responsible for:

- Reviewing the results
- Providing remediation via configuration changes or deploying security patches
- Implementing other mitigating measures
- Properly documenting any exceptions

Vulnerability remediation is to be completed as soon as possible following these guidelines:

Severity	Description	Service Level
Critical	Critical vulnerabilities have a CVSS score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits.	3 days
High	High-severity vulnerabilities have a CVSS score of 8.0 or higher or are given a High severity rating by PCI DSS v3. There is no known public malware or exploit available.	10 days
Medium	Medium-severity vulnerabilities have a CVSS score of 6.0 to 8.0 and can be mitigated within an extended time frame. 90 Days	20 days
Low	Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can’t be remediated	45 days
Information	Information vulnerabilities have a CVSS score lower than 4.0.	Not Required

	These are considered risks but are generally reference information for the state and configuration of an asset.	

These are to be reviewed and approved by the CTO and the security officer.

For more details, please see *SigningOrder_Cyber_Vulnerability_management_Policy_1.0.doc* document.

5.2.7. Audit logging (NIST CSF RP.PT-1)

Audit logging shall be enabled and configured for all production-related environments, including network, operating systems, databases, and applications.

The company is implemented AWS CloudWatch for log collection, correlation, and alerting. The application is creating security logs that are feeding into the standard Windows logs of the server.

Log sources

The following log sources collected for analysis, and alerting:

- Each server's security logs
- AWS Security Group logs
- Local Iptables logs
- Database security logs
- Application security log

Monitoring and Alerting

AWS CloudWatch is providing a powerful AI for alert correlation, and the company implemented use cases as well. The system is generating alerts and sending a notification to the operation team. The operation team is triaging the alert and, if needed, escalates to the security officer.

Incident response

The company will initiate an incident response plan after the evaluation of the collected information. Only the CEO, CTO or security officer can initiate the incident response procedure and the communication plans.

Removable media usage is not enabled in the server environment, configured via local security settings on the server.

The clients' related communication channel is encrypted, and it is only allowed via HTTPS (see Encryption section).

5.3. Detect (NIST CSF DE.)

5.3.1. Security Monitoring

AWS Inspector and Security HUB is implemented in the production environment to ensure all events are captured.

For more details, please see *SigningOrder_Security_Audit_and_Monitoring_Policy_1.0.doc* document

5.4. Response (NIST CSF RP and RS)

The company will initiate an incident response plan after the evaluation of the collected information. Only the CEO, CTO, or security officer can initiate the incident response procedure and the communication plans.

At the declaration of the incident, the team starts a log (text file, document) to record all necessary information and steps of the incident management; this log is to be used for lessons learned analysis.

The company has created and maintaining its Incident Response Plan; the response plan contains information of the recovery process. For more details, please see

SigningOrder_Cyber_Incident_Response_Plan_1.0.doc document-

DATA ENCRYPTION POLICY

Code:	SO-DEP-01
Version:	1.0
Date of version:	10-09-2019
Created by:	Attila Horvath
Approved by:	Anthony Birden
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
09-09-2019	0.1	Attila Horvath	Initial draft
09-18-20	1.0	Anthony Birden	Final version

Table of contents

1. Purpose

The purpose of this document is to define rules the use of encryption controls, the rules for the use of cryptographic keys, to protect the confidentiality, integrity, authenticity, and non-repudiation of information.

2. Scope

This policy applies to all SigningOrder LLC employees and affiliates.

3. Reference documents

- NIST CSF PR.DS.-1, DS.-2
- Information Security Strategy
- NY SHIELD ACT
- CALIFORNIA CUSTOMER PROTECTION ACT
- IETF/IRTF Cipher Catalog
- NIST FIPS 140-2

4. Definitions

Information system – includes all servers and clients, network infrastructure, system, and application software, data, and other computer subsystems and components that are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this policy, the term *information assets* are applied to information systems and other information/equipment including paper documents, cloud-based service, virtual storage, and backup solutions.

Information security – The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Encryption - Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

5. Data Encryption Policy

5.1. Policy Objectives (NIST CSF PR.DS-1, PR.DS-2)

The company must ensure the information systems used by the company are protecting data at transit, data at use, and data at rest.

5.2. Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

5.2.1. Signature algorithms

Algorithm	Key Length (min)
ECDSA	P-256
RSA	2048
LDWM	SHA256

5.3. Hash Function Requirements

In general, the company should use SHA-2 and SHA-3 functions to employ secure hash algorithms. The company should purchase services using the same methods.

5.4. Key Agreement and Authentication

Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

End-points must be authenticated before the exchange or derivation of session keys.

Public keys used to establish trust must be authenticated before use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

5.5. Key Generation

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

The key generation must be seeded from an industry-standard random number generator (RNG). For example, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5.6. Key storage

Company level cryptographic keys are protected by AWS KSM key management solution. In the case of loss, corruption, or destruction, keys are going to be recovered from the KMS.

The keys are managed by the CTO.

5.7. Servers

The server's hard drives shall be encrypted in the alignment of its performance capabilities.

5.8. SaaS solutions

The company shall select and use SaaS solutions capable of providing its services in compliance with the requirements above.

6. Implemented controls

6.1. Encryption in the production environment

6.1.1. Data at transit

SigningOrder platform is only accessible via an HTTPS connection that is terminated by Cloudflare (which also provides WAF), the website only accepts TLS 1.2 or above encryption with a limited number of chippers.

Administration access to the production environment is only possible via private keys and SSH connections, or via the AWS web interface, which is fully encrypted and using HTTPS only.

6.1.2. Data at rest

The storage volumes and the instances OS volumes are encrypted with Amazon AWS EBS encryption solution using the industry-standard AES-256 encryption methodology. Encryption keys are managed in AWS Key Management Service that is providing FIPS Level-2 validated HSM modules to store and manage the production environment's customer master key. The "customer master key" is at 32 character length and is only known by one person.

The database is also running on encrypted hard drives and storage. The MariaDB has AWS KMS plugin installed for the implementation of key management services; database encryption is configured to "everything — all tablespaces (with all tables)," temporary files are encrypted as encrypt_tmp_files=ON is set.

Backup data is synced to an encrypted S3 bucket. The platform fully encrypts all data.

Penetration testing report for SigningOrder LLC

by
Attila Horvath, CISA, CISSP

Executive Summary

Attila Horvath was contracted by SigneingOrder.com LLC to conduct a penetration test to determine exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against SigningOrder.com LLC with the goals of:

- o Identifying if a remote attacker could penetrate SigningOrder.com LLC defenses

Determining the impact of a security breach on:

- o Confidentiality of the company's private data
- o Flaws or weakness of the web applications of SigningOrder.com LLC

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151, with all tests and actions being conducted under controlled conditions.

Scope

SigningOrder.com website.

Summary of results

The initial reconnaissance of the targets revealed minimal information and no vulnerabilities on the hosts. The investigation carried out with hand and automated tools only identified necessary information about the hosts. The website only responded to HTTPS the HTTP traffic is redirected to HTTPS. Only low-level vulnerabilities identified and

Attack narrative

Identification of the host, IP addresses:

Address lookup

canonical name	signingorder.com.
aliases	
addresses	104.26.7.148 104.26.6.148 2606:4700:20::681a:694 2606:4700:20::681a:794

Testing results for SigningOrder.com websites:

Identified vulnerabilities

There were only three vulnerabilities identified with minimal vulnerability score, two relating to the webserver (Apache) configuration, and one relating to cookie configuration.

Verbose error message

CWE CWE-693
OWASP A6 Security Misconfiguration
WASC WASC-15 APPLICATION MISCONFIGURATION
CVSS Base 5 CVSS Temporal 4.1

Details

Threat
The X-Frame-Options header is not set in the HTTP response, which may lead to a possible framing of the page. An attacker can trick users into clicking on a malicious link by framing the original page and showing a layer on top of it with legitimate-looking buttons.

Impact
Attacks such as Clickjacking could potentially be performed.

Solution
The "X-Frame-Options:" allows three options DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to set "X-FRAME-OPTIONS to DENY" which won't allow any domain to frame the site or SAMEORIGIN which only allows framing by the same site. DENY and SAMEORGIN are supported by all browsers. Setting "X-FRAME-OPTIONS" to ALLOW-FROM may still leave users vulnerable to Clickjacking since not all browsers support ALLOW-FROM including CHROME and SAFARI. For more information, see
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet.

Conclusion: However, it is recognized as a vulnerability it poses no real threat as the server is not responding.

Application misconfiguration – Low

OWASP A6 Security Misconfiguration

WASC WASC-15 APPLICATION MISCONFIGURATION

Details

Threat
No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade

3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution
Referrer Policy header improves security by ensuring websites will not leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Conclusion: This is a low-level information gathering vulnerability,

The Feature-Policy response header is not present.

OWASP	A6 Security Misconfiguration
WASC	WASC-15 APPLICATION MISCONFIGURATION

Details
Threat
The Feature-Policy response header is not present.
Impact
Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.
These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.
Solution
It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.
References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Conclusion: This is a low-level information gathering vulnerability,

SECURITY RISK MANAGEMENT

Code:	SO-SRM-01
Version:	Final
Date of version:	11-17-2019
Created by:	Attila Horvath
Approved by:	Anthony Birden
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
10-28-2019	0.1	Attila Horvath	Initial draft
11-17-2019	1.0	Anthony Birden	Final version

Table of contents

1. Introduction

1.1. Purpose

All activities undertaken by the Company carry an element of risk. The exposure to these risks managed through the practice of Risk Management. In managing risk, it is the Company's practice to take advantage of potential opportunities while managing potential adverse effects.

1.2. Scope

Managing risk is the responsibility of everyone in the Company. This policy outlines the Company's risk management process and sets out the responsibilities of conducting Risk Management activities.

2. Reference documents

- NIST CSF ID.GV-4, ID.RM, ID.RA
- NIST RMF (800-37 rev2)
- NIST 800-30

3. Definitions

Information system – includes all servers and clients, network infrastructure, system, and application software, data, and other computer subsystems and components that are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, and other services.

Information assets – in the context of this policy, the term *information assets* are applied to information systems and other information/equipment, including paper documents, cloud-based service, virtual storage, and backup solutions.

Risk – A measure of the extent to which a potential circumstance or event threatens an entity and typically is a function of (i) the adverse impact or magnitude of the harm that would arise if the condition or event occurs; and (ii) the likelihood of occurrence.

Probability – A weighted factor based on a subjective analysis of the likelihood that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Risk assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and resulting from the operation of a system.

Risk management –The program and supporting processes to manage risk to organization operations (including mission, functions, image, reputation), organization assets, individuals, other

organizations, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Security – A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.

4. Risk Management

4.1. Risk Management policy

It is the policy of the Company to perform an annual assessment of its operation that identifies threats, vulnerabilities. It results in a formal risk assessment and documents the results of the risk assessment in a report.

The scope of the risk assessment shall include all business processes, technologies, personnel, facilities, and any business associates who are participating in the operation.

The CTO is responsible for the *Risk Assessment Process* and documentation of the results. The risk assessment report includes the description of all information security-related risks, and the assessment of the currently implemented controls to manage the risk.

Not all risks can offset at a cost commensurate with the assets to be protected; however, it is not only legitimate but also prudent for management to accept certain levels of risk as a "cost of doing business."

Risks described as a combination of the consequences of an event occurring and its likelihood of occurring.

Risk is the chance of something happening that has an impact on objectives and risk management described as the culture, processes, and structures that directed towards realizing potential opportunities while managing an adverse effect.

The Company's risk management system designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to the Company.

The Company is managing risks related to its general operation, and risks which are associated with specific projects so-called "project risks," the assessment process is used in both cases but on different scales.

The company risk acceptance criteria or risk appetite is "Low."

4.2. Risk Assessment

A risk assessment is used by organizations to identify threats and vulnerabilities that could negatively impact the security of the operation activities. This policy guides in creating a formal risk assessment process to identify, analyze, and document the risks that may affect the environment.

The risk assessment applies to all the SigningOrder.com LLC's business processes, technologies, personnel, facilities, and any business associates participating in operational activities.

The Company shall implement a risk-assessment process that is performed at least annually in the environment and upon significant changes to the operational procedures (for example, acquisition, merger, relocation, or other significant changes.). The process shall identify critical assets, threats, and vulnerabilities, and result in a formal risk assessment.

The Company implemented the risk assessment methodology described in NIST SP 800-30 publication. The assessment method for SigningOrder.com LLC's is qualitative, and the analysis approach is asset/impact-oriented.

4.2.1. Risk Assessment Process

SigningOrder.com LLC's shall establish a Risk Assessment Process that incorporates the following core activities:

- Identify critical assets and the threats to those assets;
- Identify single points of failure within the information systems infrastructure;
- Identify vulnerabilities; both organizational and technological that could potentially expose assets to those threats, resulting in a risk to the organization;
- Prioritize essential business functions;
- Develop a risk strategy and risk mitigation plan to address identified risks in support of the organization's mission and priorities.

The Risk Assessment Process must include the following:

- Procedures to prevent, detect, contain and correct security violations;
- Addresses security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;
- Addresses all compliance requirements;
- Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment;
- Consists of a review at least annually and updates when the environment changes.

4.2.2. Critical Assets Identification

Critical assets include the people, processes, and technologies that are involved in the processing, storage, transmission, and protection of sensitive data. Each critical asset must be assigned an Impact Category to characterize the level of severity the Company should the asset become unavailable.

Impact categories include High, Medium, and Low.

SigningOrder.com LLC's CTO maintains the list of critical assets. For asset identification and management policy, please see the Asset Management and Classification Policy and the Data Classification Policy 1.0.

4.2.3. Threat Identification

Threats may include people, the systems they use, and conditions that could cause harm to the Company. Review security incidents that may have occurred within the Company or industry to identify potential threats.

The CTO maintains the list of threats.

4.2.4. Vulnerability Identification

Vulnerabilities are weaknesses that can be exploited by a threat and may originate from technology, the Company, the environment, or a business process. Vulnerabilities can occur as a result of the design, development, or deployment deficiencies of systems or software. Organizational and business-process vulnerabilities may exist because of non-existent or ineffective policies and procedures. Vulnerabilities identified from vulnerability assessment reports, penetration-test reports, and technical security audits such as firewall rule reviews, secure code reviews, and database configuration reviews.

The CTO maintains the list of vulnerabilities.

4.2.5. Existing Controls

Existing controls are those that are already present in an organization to protect against the identified threats and vulnerabilities. Review existing policies/procedures, interview people, observe processes, and review previous audit reports and incident logs to determine the adequacy of existing controls.

4.2.6. Risk Tolerance

Risk tolerance is the level of risk that the Company is willing to assume to achieve a potential desired result. It is the CTO's responsibility to define the risk tolerance level of the Company.

4.3. Risk Assessment tool

The Company is using an Excel-based Risk Assessment Tool, which is developed based on the NIST 800-30 methodology.

The tool is available to the authorized users at the "/Security/Risk Assessment" folder at the Company's Google Drive as a google sheet. SigningOrder Risk Assessment Tool.xlsx

4.4. Risk treatment plan

After the risks have identified and evaluated, the CTO develops a risk mitigation plan, which is a plan to reduce the impact of an unexpected event. Mitigation of risks can be done in the following ways:

- Risk avoidance,
- Risk acceptance,
- Risk reduction,
- Risk transfer

Each of these mitigation techniques can be a useful tool in reducing individual risks and the risk profile of the Company. The risk mitigation plan captures the risk mitigation approach for each identified risk event and the actions the senior management team take to reduce or eliminate the risk.

Risk avoidance usually involves developing an alternative strategy that has a higher probability of success but usually at a higher cost associated. A common risk avoidance technique is to use proven and existing technologies rather than adopt new techniques, even though the new techniques may show promise of better performance or lower costs.

Risk acceptance is accepting the risk and determining that it is within the Company's risk tolerance.

Risk reduction is creating controls to reduce or eliminate the risk.

Risk transfer is a risk reduction method that shifts the risk from the project to another party. The purchase of insurance on certain items is a risk transfer method. The risk transferred from the Company to the insurance company.

The risk treatment plan should contain the selected risk management option for each of the risks and the steps of how it delivered/executed, as well as defines the residual risk. It is the responsibility of the CEO to validate if the amount of residual risk is in line with the Company's risk tolerance level. The CEO must approve of the risk treatment plan.

The senior management is responsible for establishing a process to monitor the risk treatment plan execution.

5. Appendix A – Risk Assessment process guide

The risk assessment method and approach are based on qualitative risk assessment use a scale to associate a value to the risk elements from low to high.

The CTO records the asset identification into the Asset identification and classification google sheet, which located at the "/Security/Asset register" folder.

Each asset is classified and evaluated for the CIA attributes. The asset list approved by the CTO, CEO, and departmental leaders.

The risk assessment process is a 4 step process:

1) Asset selection of the affected department from a drop-down menu, identification of the Risk Owner, selection of the asset from a drop-down menu, and choice of the location from a drop-down menu.

Risk ID	Department	Owner Contact	Asset	Location(s)
1	Whole Organization	CEO	Physical assets in the office	Madrid Office
2	Whole Organization	CEO	Physical assets in the office	Madrid Office
3	Whole Organization	CEO	Physical assets in the office	Madrid Office

2) Selection of the affected parties (Customers, Employees, Vendors, Clients, Notaries), Selection of the Threat from a drop-down menu, Selection of the Vulnerability from a drop-down menu, and selection of the Impact description of the drop-down menu.

Affected	Threat	Vulnerability	Impact Description
Employees, Customers	Fire	Inadequate physical protection	Fire in the office destroys the assets in the office
Employees, Customers	Errors in maintenance	Inadequate physical protection	Unfavourable climatic conditions like heat, frost or high humidity can lead to a wide variety of damage, like malfunctions in technical components or damage of storage media.
Employees, Customers	Flood	Location vulnerable to flooding	Water can affect the integrity and availability of information stored on analogue and digital data storage media.

3) Selection of the probability and impact values, the Overall risk value is calculated automatically. These are raw values without any mitigations or controls.

Risk Exposure

Risk Exposure is calculated by multiplying the Probability Level by the Impact Level.

Heat Map: ***Image of Risk Exposure***

Business Impact						
	10 Catastrophic	10 Low	30 Medium	50 High	70 High	100 High
	7 High	7 Low	21 Medium	35 Medium	49 High	70 High
	5 Medium	5 Low	15 Medium	25 Medium	35 Medium	50 High
	3 Low	3 Low	9 Low	15 Medium	21 Medium	30 Medium
	1 Insignificant	1 Low	3 Low	5 Low	7 Low	10 Low
		1 Rare	3 Unlikely	5 Possible	7 Likely	10 Certain
		Probability				

[5] Heat Map Guidelines

Low
Medium
High

Risk Definition

Low risk means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals.

Medium risk means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals

High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

After the overall risk calculated, the CIA attributes needed to be selected; this is done based on the Asset register CIA attributes but can be changed. The risk appetite value is by default LOW for SigningOrder.com LLC's, meaning that the Company could accept overall raw risks defined low, but medium and high overall risks are must be mitigated.

Probability	Impact	Overall Ri	Confidentiality	Integrity	Availabili	Risk Appetite
3	7	21	**Low**	**Low**	**High**	Medium
3	7	21	**Low**	**Low**	**High**	Medium
3	7	21	**Low**	**Low**	**High**	Medium

4) The final step is to define mitigation control and set residual probability and impact values.

Risk Mitigation	Residual Likelihood	Residual Impact	Overall Residual Risk	Risk Level
Fire alarm system, smoke detectors	1	1	1	**Low**
Facility management in place monitoring office conditions	1	1	1	**Low**
Facility management in place monitoring office conditions	1	1	1	**Low**

In the case that no mitigation factor is in place, it is the CTO's responsibility to research and propose mitigations and create the risk treatment plan.

DISASTER RECOVERY PLAN

Code:	SO-DRP-01
Version:	1.0
Date of version:	01-17-2020
Created by:	Attila Horvath
Approved by:	Anthony Birden
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
01-06-2020	0.1	Attila Horvath	Initial draft
01-17-2020	1.0	Anthony Birden	Final version

Table of contents

1. Purpose

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes SigningOrder.com LLC's ability to withstand a disaster as well as the processes that must be followed to achieve recovery from a disaster.

The goal of the document is to guide the steps in a Disaster Recovery scenario to restore services to business-as-usual as quickly as possible. It includes:

- Preventing the loss of the organization's resources such as data and logical IT assets
- Minimizing downtime of the services provided by the company
- Keeping the business running in the event of a disaster
- This DRP document details how this plan is to be maintained and tested.

2. Scope

All employees of SigningOrder.com LLC, herein referenced to as "Company", must comply with the terms of this policy immediately. The production environment is running at the AWS North Virginia Region and the AWS storage solution in the same region but different availability zone where daily backups and database backups are stored.

3. Reference documents

ISO 22301:2019 Business continuity management systems

ISO 22300:2018 Security and resilience — Vocabulary

ISO 31000:2018 Risk Management Guidelines

4. Definitions

Information system – includes all servers and clients, network infrastructure, system, and application software, data, and other computer subsystems and components that are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this Policy, the term information assets is applied to information systems and other information/equipment, including paper documents, cloud-based service, virtual storage, and backup solutions.

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of (i) the adverse impact or magnitude of the harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and resulting from the operation of a system.

Risk management –The program and supporting processes to manage risk to organization operations (including mission, functions, image, reputation), organization assets, individuals, other organizations, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Security – A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery and correction that should form part of the organization's risk management approach.

Disruption – incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives

Business Continuity Plan (BCP) – A comprehensive written plan to maintain or resume business in the event of a disruption.

Business Impact Analysis (BIA) – The process of identifying the potential impact of uncontrolled, nonspecific events on the business processes.

Data Redundancy – Production server performs full virtual machine replication between the production data center and secondary instance every 15 minutes

Disaster Recovery Plan – A plan that describes the process to recover from major processing interruptions.

Emergency Plan – The steps to be followed during and immediately after an emergency such as a fire, tornado, bomb threat, etc.

Encryption – The conversion of information into a code or cipher.

Replication – A process that duplicates data to another location over a computer network in real-time or close to real-time.

Recovery Point Objectives – The amount of data that can be lost without severely impacting the recovery of operations.

Recovery Site – An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as "hot" sites that are fully configured centers with VPN access to our data centers and "cold" sites that are operational centers without VPN connectivity to remote data centers.

Recovery Time Objectives – The period that a process can be inoperable.

Recovery Vendors – Organizations that provide recovery sites and support services for a fee.

5. Disaster Recovery Planning

5.1. General

The organization is committed to ensuring the availability, security, and integrity of customers' information and its services by continually improving and adapting to meet ever-evolving security and availability demands. The company uses multiple faceted approaches to protect clients' interests and is continuously monitoring the production environment.

5.2. Definition of a disaster

A disaster can be caused by man or nature and results in [Company] not being able to perform all or some of their regular roles and responsibilities for some time.

The company defines disasters as the following:

- One or more critical systems are non-functional
- AWS Region Data Center services are not available

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- Fire
- Flash flood
- Pandemic
- Power Outage
- War
- Theft
- Terrorist Attack
- Ransomware/Virus

5.3. Disaster Recovery Teams and responsibilities

The company's staff is located in the US, but working only remotely, as a virtual team. The following virtual team has been identified.

5.3.1. Disaster recovery team

Team member name & DR Responsibility	Email	Phone number
Anthony Birden	Anthony.birden@notaryloop.com	
Aaron Johnson	Aaron.johnson@signigorder.com	

5.4. Plan activation and deactivation

Activation of the business continuity plan is automatically done in a case when a disaster recovery incident is declared by the CEO. The plan is deactivated after the incident is declared to be solved. The plan activation communication can be written and/or oral.

5.5. Communication plan

In a case when the DR plan is activated, the CEO is the only authorized person to communicate the case with the public, authorities, and with the clients. The CEO will inform clients within the SLA or the contractual requirements defined with each client.

5.6. SigningOrder.com LLC Production Cloud - Base Production Configuration

The production environment is created in the AWS North Virginia Region, availability zone is us-east-1f, backups are stored in an encrypted S3 bucket in the same region, but the availéability zone is us-east-1d.

AWS availability zones are located in the same AWS region but two different data centers. The availability zones are connected with low latency networks.

The SigningOrder platform is protected by Cloudflare WAF solution, and AWS Security Groups are configured as the edge firewall protecting all internal network segments.

The backend database is a MariaDB provided by AWS RDS service. Amazon RDS synchronously replicates the transaction log of the database to us-east-1d availability zone.

The virtual machines serving the Web Application servers and the Database servers are running CentOS.

5.7. SigningOrder.com LLC Production Cloud – Backup

5.7.1. Running environment

Backups are configured in the production environment to ensure data availability- Image snapshots of the servers are created every day and stored at AWS Availability zone us-east-1d encrypted S3 bucket.

5.7.1. MariaDB Database

The database transaction log is continuously synced to the encrypted S3 bucket in the separate S3 bucket. The end of the day backup of the database is also synced to the encrypted S3 bucket.

5.7.2. High-level architecture diagram

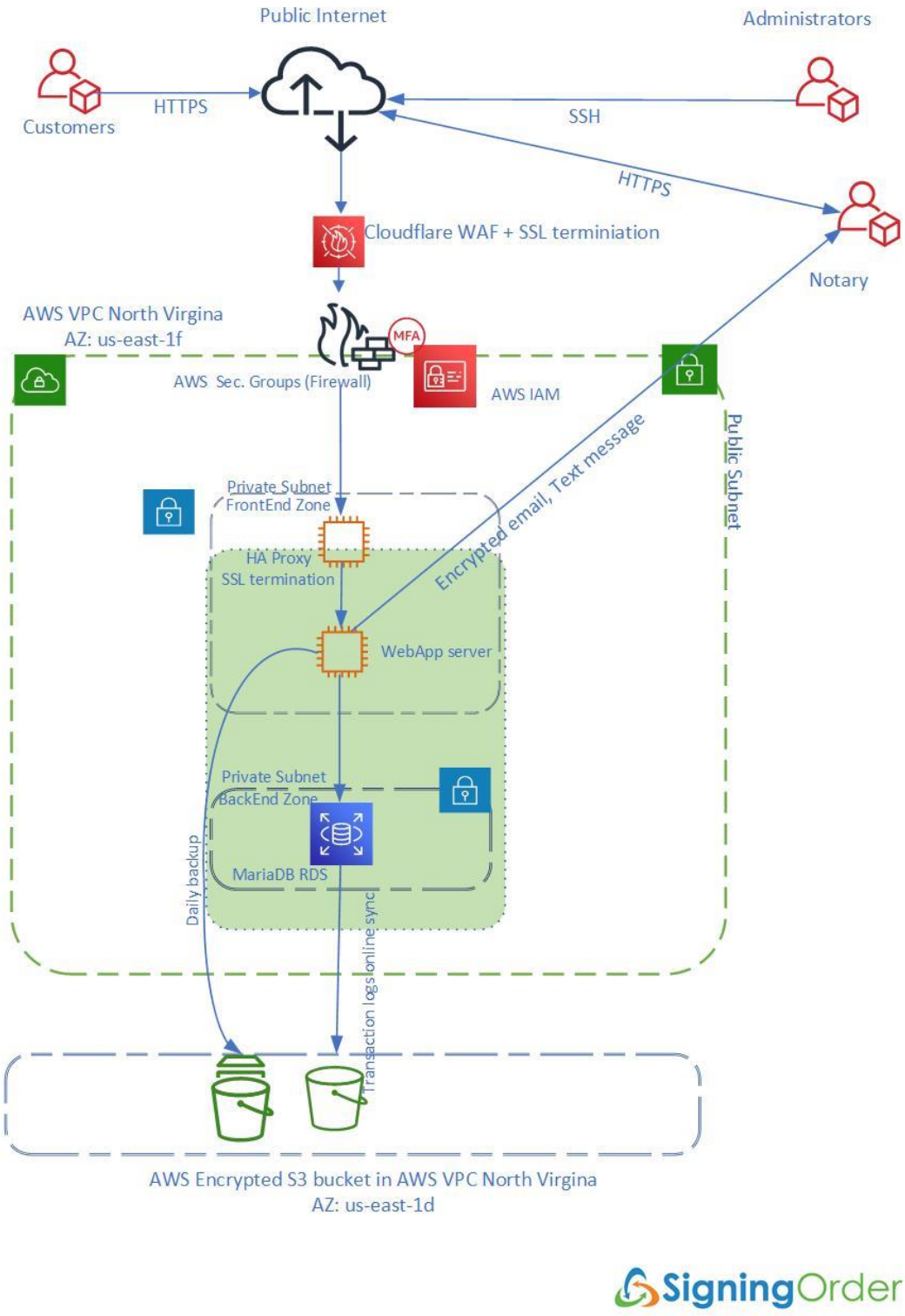


Figure 1 - High-level AWS architecture

5.7.3. Detailed backup schedule

The detailed backup schedule is the following:

Instance name	Availability zone	Backup size	Backup Location	Backup time
Webapp01	AZ US East 1F	50 GB	AWS S3 bucket	01:00 am daily
MariaDB01	AZ US East 1F	25 GB	AWS S3 bucket	01:00 am daily
MariaDB01 transaction log	AZ US East 1F	Continuous sync	AWS S3 bucket	Ongoing

All backups are transferred and stored encrypted; the encryption keys are managed with AWS KMS solution by the security officer. Backup integrity is validated manually by the IT operation team every 180 days, and a ticket is created about the task.

5.8. SigningOrder.com LLC Production Cloud - RTO and RPO

The company has conducted a Business Impact Analysis and defined the Recovery Point Objective to 4 hours, as the database is backed up at every 4 hours the company meets it's RPO goal.

The RTO is defined for the loss of the whole AWS availability zone; in this case, the complete production environment needs to be restored from backups to another AWS Region or Cloud Service Provider.

RTO	Time to recover
HIGH	24 hours
MEDIUM	48 hours
LOW	5 days

RPO	Recovery point
HIGH	0 mins
MEDIUM	24 hours

LOW	72 hours

5.9. SigningOrder.com LLC Production Cloud - DR procedure

5.9.1. Availability Zone related scenarios

In the case, if the AWS availability zone services (network, storage,) become unavailable, the operation team will move the production EC2 instance to another availability zone within the region via the AWS management console.

Configuration of the Cloudflare WAF and SSL certification also needs to be carried out.

5.9.1. AWS Region related scenarios

In the case, both the AWS Availability zone and AWS service within the region or worldwide become unavailable, full data and environmental restoration are needed. The CEO invokes the DR Plan and notifies the technical team to start the DR procedures.

5.9.2. Detailed DR steps for AWS hosted system

In the case of AWS services are available for the AZ US EAST 1d region and the Backups S3 buckets can be accessed, it should be the primary source for the restoration process of the running environment. If AWS BBB Region is unavailable, the backups from the offsite storage solution must be used.

In the case that AWS service is not available, the system will be restored to Google Could Provider. The cost of the services will be covered by the COO role, SigningOrder.com LLC bank card. If the company bankcard is not possible to use, the personal source will be used for the setup, which amount will be reimbursed.

The detailed confidential restore document is located at the company's google drive under "/Security/DRP/".

5.10. Plan Testing & Maintenance

While efforts made initially to construct this DRP in a complete and accurate a manner as possible, it is virtually impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the company will change. As a result of these two factors, this plan needs to be tested periodically to discover errors and omissions and need to be maintained to address them.

5.11. Maintenance

The DRP will be updated annually, or any time a major system update or upgrade is performed, whichever is more often. The CISO responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization to complete this task.

Maintenance of the plan include (but is not limited to) the following:

- Ensuring that all team lists are up to date
- Reviewing the plan to ensure that all the instructions are still relevant to the organization
- Making any major changes and revisions in the plan to reflect organizational shifts, changes, and goals
- Ensuring that the plan meets any requirements specified in new laws
- Other organizational specific maintenance goals

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the CTO to appoint a new team member.

5.12. Testing

SigningOrder.com LLC is committed to ensuring that this DRP is functional. The DRP should be tested every 12 months to ensure that it is still valid. Testing the plan will be carried out as follows:

Walkthroughs - Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a more significant subset of people, allowing the CISO to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities

Simulations - A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Parallel Testing - A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

Full-Interruption Testing - A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence concerning previous DRP phases cannot be overstated.

Any gaps in the DRP that are discovered during the testing phase will be addressed by the CISO, as well as any resources that he/she will require.