INTERNAL USE ONLY

24 EXCHANGE

INFORMATION SECURITY AND CYBER RISK POLICY & PROGRAMME

REVISED AS OF

MAY 1, 2023

INFORMATION SECURITY AND CYBER RISK POLICY & PROGRAMME

The following Information Security and Cyber Risk Policy & Programme is the sole property of 24X Bermuda Holdings LLC (Parent) and its affiliates and subsidiaries (collectively, "24 Exchange" or the "Company").

Introduction

This policy defines:

- Information security objectives of 24 Exchange
- Roles and responsibilities
- Security guidelines and requirements for 24 Exchange information technology assets
- Security Awareness Training (currently via Thompson Reuters Compliance Learning)
- Authority & Access Control
- Data Support and Operations
- Disciplinary Actions

Information Security Objectives

Create and strengthen all internal security controls and prevent unauthorizedand improper access to data by securing and ensuring the appropriate protection of information technology assets and data. All policies aim to preserve the following:

- Confidentiality - Access to data shall be confined to those with the appropriate authority.
- Integrity - Information shall be complete and accurate. All systems,assets and networks shall operate correctly and according to specification.
- Availability - Information shall be available and delivered to the rightperson when it is needed.

Understanding Cybersecurity

Cybersecurity risks are a real threat to all businesses, regardless of size or industry. Cybersecurity is treated as a strategic risk which is addressed at all levels of 24 Exchange, including Board level. Cyberattacks are frequently crimes of opportunity. The risk of a cybersecurity breach can be greatly reduced through the measures set out in this Policy.

Cybersecurity threats may come in the form of targeted cyberattacks on particular targets (such as distributed denial of service (DDoS) attacks) or indiscriminate threats (such as phishing). They are carried out by a range of businesses and individuals, including:

- Organised crime networks seeking to profit from the unlawful use or sale of data.
- Hostile governments aiming to obtain defence secrets.
- Politically motivated hackers and groups whose mission is to reveal shortcomings in governments and private companies.

24 Exchange takes the three lines of defense approach as set out in this Policy:

(i) first-line operational controls.

24 Exchange maintains an evolving cyber security policy with attention to continuous improvement. The potential for internal risks is understood, and mitigated by careful vetting of all personnel, and continuous testing of software and systems. Electronic systems are protected by keeping servers in highly secure data centers which are monitored 24/7. The information stored on the firm's electronic systems is also secured by means of adherence to the firm's IT security policy.

The detection of system intrusions and breaches is part of a comprehensive plan to revise and expand the firm's IT security defenses. There are existing logging facilities in place presently which would serve as a basis for a post-breach forensic analysis, and there are other advanced measures taken by Lucera and Equinix. The following facilities address logging, and the detection of intrusions and breaches:

Graylog is used to collect and store all system logs from all servers.

Snort IPS is used on company routers to monitor network traffic anomalies, help define malicious network activity and generate alerts.

pfBlock-NG provides advertisement and malicious content blocking along with geo-blocking capabilities.

Lynis is used for vulnerability detection and systems hardening.

(ii) second-line IT risk identification and management.

24 Exchange maintains a Risk Management Policy, which outlines the process it will use to identify IT risks and associated controls. 24 Exchange also conducts penetration tests, either internally or through a third-party vendor. The Exchange contracted with Rhymetec to conduct penetration testing in November 2022. From the November test, 7 low to medium vulnerabilities were identified. Six of seven were fixed, and the risk score was reduced from moderate to low in a follow-up pen test in December 2022.

(iii) third-line independent cyber risk audit[1].

Regulatory Obligations

24 Exchange and the Chief Information Security Officer are familiar with the Bermuda Virtual Currency (Cybersecurity) Rules 2018 and will annually file with the Bermuda Monetary Authority a written report prepared by the Chief Information Security Officer assessing—

a. the availability, functionality and integrity of its electronic systems;
b. identified cyber risk arising from any virtual currency business carried on or to be carried on, by the licensed undertaking; and
c. the cyber security program implemented and proposals for steps for the redress of any inadequacies identified.

[1] (i)24 Exchange has engaged Vanta for ISO 27001 certification which includes a cyber risk audit by an independent third-party firm. It is anticipated that ISO 27001 certification will be issued during Q1/Q2 2023.

Roles and Responsibilities

President

24 Exchange has a President who is also the Chief Information Security Officer of the company. President is responsible for enforcing all informationsecurity policies.

CEO

24 Exchange has a CEO who is responsible for making sure the Chief Information Security Officer is enforcing all policies.

Chief Information Security Officer

The Chief Information Security Officer (CISO) is currently Jason Woerz, who is responsible for ensuring security.The Chief Information Security Officer will:

- Create and manage departmental security policies
- Coordinate audits to make sure security policy is being enforced
- Coordinate 24 Exchange's incident response team
- Represent the department on the 24 Exchange Security Team
- Oversee data privacy compliance
- Communicate new or revised policies, procedures, and standards onbehalf of the Security Team to all employees

Security Team

The Security Team includes:

- Jason Woerz, President, CISO
- David Sassoon, General Counsel,
- Roli Bhotika, COO, Technology,
- Andrey Golik, Software Developer,
- Jeremy Sanchez, Chief Compliance Officer, and
- Doug Paratore, Systems Administrator.

This team develops, updates, and approves security policies, related procedures, and related standards. During this process, the team considers the business needs and security concerns of 24 Exchange. The team also reviews any deviation from standards/policies and then approves or denies the exceptions.

All Employees

All authorized users, staff members, employees, consultant volunteers, and contractors (collectively "employees") who have access to 24 Exchange resources must:

- Read, understand, and follow all 24 Exchange policies relevant to their roles and responsibilities
- Help protect 24 Exchange data and resources from being shared orchanged without permission

Security Guidelines and Requirements

- All members of 24 Exchange must have access to the security policies,and procedures relevant to their roles and responsibilities.
- These policies, procedures, and standards must comply with and support applicable laws, regulations, and contracts.
- The Security Team must approve any exceptions to the minimum-security requirements and make sure compensating controls exist.

Security Awareness

To make sure all users are familiar with security, Chief Information SecurityOfficer must:

- Implement training on best practices in information security, commonthreats, reported incidents, and the secure use of information security assets
- Add security awareness to new employee orientation materials
- Supply 24 Exchange management with feedback on an employee's security awareness, which will be used in that employee's evaluation
- Review this program annually in order to update it for changes in technology and security needs

Authority & Access Control

Authority and access control will be reviewed to ensure only the properaccess is given to relevant parties. This includes access to:

- Information
- Information technology assets
- Systems
- Software
- Networks

Data Support and Operations

By establishing the above guidelines in the Information Security Policy and following all other associated policies, 24 Exchange incorporates security by design into its data support and operations.

Audit

24 Exchange has established audit trail systems that:

a. track and maintain data which allows for the complete and accurate reconstruction of all financial transactions and accounting;
b. protect the integrity of data stored and maintained as part of the audit trail from alteration or tampering;
c. protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;
d. log system events including but not limited to access and alterations made to the audit trail systems;
e. maintain records produced as part of the audit trail.

24 Exchange will engage a qualified independent party to audit its systems and provide a written opinion to the Bermuda Monetary Authority that the cyber security program is suitably designed and operating effectively to meet the requirements of the Virtual Currency (Cyber Security) Rules 2018[2].

Disciplinary Actions

- Employees who don't follow all applicable policies may face disciplinary action, such as denial of access, legal penalties, and/or dismissal.
- Any employee aware of a violation of these policies must report it to asupervisor or other authorized representative who must in turn report to the Chief Information Security Officer.
- If employees or third parties want to be exempt from any part of thispolicy, they must first get permission (in writing) from the Chief Information Security Officer.

Sub Policy – 24 Exchange Data Classification and Access

This policy defines 24 Exchange's data classification levels and Access. Thelevels determine who has permission to access 24 Exchange's data and underwhat conditions. This policy helps us because:

- When everyone classifies data appropriately, the Security Team will beable to protect it with the security measures that apply to that classification level.
- If you understand these data classification levels, you will know whether or not you have permission to read, share, change, or deleteinformation.

[2] 24 Exchange has engaged Vanta for ISO 27001 certification which includes a cyber risk audit and report. It is anticipated that ISO 27001 certification will be issued during Q1/Q2 2023.

When everyone has this common understanding and follows this policy, 24Exchange will be less likely to experience harmful data leaks.

Understand the Information Categories

What is Confidential Data?

Confidential - Data needing the most limited access and which must maintain its integrity. This data will do the most damage to 24 Exchange if itis leaked or accessed without authorization.

What is Internal Data?

Internal - Data that is disclosed outside the company on a limited basis or contains information that could reduce 24 Exchange's competitive advantage

What is Public Data?

Public - All other information that does not clearly fit into any of the other classifications. Sharing public information without authorization should not seriously or negatively affect 24 Exchange. However, employees should stillask for permission from the Chief Information Security Officer before releasing public data.

Restrict Data Access Based on Its Category

24 Exchange will protect all data to make sure that no one improperly discloses it, modifies it, deletes it, or makes it unavailable. 24 Exchange will:

- Start logs of who accesses 24 Exchange servers and when.[3]
- Set up a process for employees to formally request access to systems or applications that handle 24 Exchange data.
- Make sure that the Chief Information Security Officer or the Security Team is responsible for approving or denying the Data Access requests.

[3] Logs are currently maintained for 30 days.

Data Breach Reporting

All Employees must report any data breaches irrespective of the level of Severity (defined in later sections) immediately to the Security team which will assess and report to the Chief Information Security Officer of any clients who may be impacted. Chief Information Security Officer (CISO), which is currently Jason Woerz, will then initiate the process of contacting the clients who may be at risk of any data breach.

Sub Policy – 24 Exchange Risk Assessment

Introduction

This policy specifies when to perform risk assessments of equipment, systems, and data systems. The policy also outlines who is responsible forthis ongoing process of discovering, identifying, correcting, and preventing potential security problems. A strong Risk Management Policy helps 24 Exchange determine and resolve security weaknesses before someone exploits them.

Roles and Responsibilities

Security Team

The Security Team member should be familiar with computer security and technology. The team must:

Perform risk assessments on 24 Exchange equipment and systems.

- Run Penetration Testing of the electronic systems and vulnerability assessment of those systems at least on an annual basis and more often, as needed.
- Develop, manage, communicate, and enforce a risk assessment framework.
- Promote good risk management strategies at 24 Exchange.

Chief Information Security Officer (CISO)

The Chief Information Security Officer must keep up-to date on:

- Technology
- Security threats
- Mitigation methods

In the context of risk assessment, the Chief Information Security Officer:

- Makes sure that the Security Team performs risk assessments promptly.
- Has the authorization to shut a service down if it poses a serious securityrisk.
- Must keep up-to-date on technology, security threats, risk mitigationmethods
- Ensures that a risk register identifying and tracking cyber risks is kept

All Employees

All Employees must cooperate during risk assessments of any systems orequipment they're responsible for.

Responsible Parties

After receiving the risk assessment report, the responsible parties mustresolve any security issues it identifies.

When to Perform Risk Assessments

Risk Assessments will be conducted in accordance with the Risk Management Policy, which includes a procedure for conducting risk assessments.

Sub Policy - 24 Exchange Incident Response

Introduction

This policy explains how 24 Exchange quickly resolves security incidentsreported to The Security Team.

24 Exchange will follow this policy for all incidents, especially when anincident affects a critical system.

The Security Team or Chief Information Security Officer may allowexemptions to this policy, but it must be approved in writing.

Accept Incident Reports

At least one member of the 24 Exchange Security Team must be available toinitiate the incident response plan at any time of day or night.

Employees may receive incident reports in two ways:

1. Automated Security System Notifications
2. Email from the CEO, President or Chief Information Security Officer.

Employees must review the Incident Response Procedure (below), so that theycan support personnel through the reporting process. The policy encourages employees to report any suspicious activity and reassures the reporters thatit's better to report innocent activity than to ignore a serious security breach.

Make sure that all incident reporters keep the incident confidential. The Security Team will coordinate all communications with external parties, suchas clients, law enforcement, or the public.

Classify the Incident Severity

The first step is to determine whether the security incident justifies a formalincident response. To determine the appropriate plan, classify the incident severity:

Severity 3:

- One instance of possible malicious activity

Severity 2:

- Any attempt to obtain unauthorized information or access
- Two **Severity 3** incidents
- Any incident involving Confidential or Sensitive data
- Any incident originating from an unauthorized *internal* system

Severity 1:

- A serious attempt to breach security
- An actual breach of security
- Two **Severity 2** incidents

See below for the full incident response plans for each threat level.

Follow the Incident Response Plan

After identifying and classifying an incident, these procedures will befollowed by Information Security team.

Incident Response Procedure:

Severity 3: Contain and Monitor

24 Exchange team will contain the situation and monitor it to see whetherthere's an actual security threat.

Severity 2: Contain, Monitor, and Warn

In addition to containing and monitoring the situation, security team will alsoneed to notify management and affected parties.

Severity 3: Contain, Eradicate, Recover, and Perform Root CauseAnalysis

In addition to the Severity 3 and 2 steps, Security team will work to eradicatethe threat, recover lost data where possible, and perform a root cause analysis.

See below for additional details pertaining to different types of securityincidents.

Physical Security

If the incident involves physical security, such as possible theft or unauthorized access:

Severity 3 Incidents: Contain and Monitor

- A member of the Security Team will review physical security checks, such as security footage and access logs, and make copies. Keep thesecopies in a different location from the originals.
- Inventory the secure location. Is anything missing/replaced? Is theresomething new present (e.g., suspicious USB key that could containmalware)?
- Try to determine whether a missing item has just been misplaced /logged incorrectly.
- Determine whether an intruder intended to access an area requiring authorization. i.e., Was this a communication error or a misunderstanding? If so, how did the intruder get through the physicalsecurity measures? Block that entry.

Additional Step for Severity 2 Incidents: Warn

- Let physical security or front desk personnel know about the situationso that they can be more aware of this type of unauthorized access.
- In the case of theft, you may begin to coordinate with law enforcement.
- Notify and keep management updated about the incident.
- Assess whether you should reclassify the incident.

Additional Steps for Severity 1

- *Eradicate:* Block the method of unauthorized entry.
- *Recover:* Determine what kind of damage has been done or could be done based on the physical security incident. If the secure location hosts backup drives or servers, ensure they haven't been damaged in any way. If data has been lost, follow the Disaster Recovery/ BusinessContinuity procedures.
- *Perform Root Cause Analysis:* Do the security cameras have enough coverage of the facility? Does the visitor log work effectively? Shouldsecurity guards increase their rounds in that area of the facility?

Network Security

If the incident involves a possible or actual attacker on the network:

Severity 3 Incidents: Contain and Monitor

- Record as much information as you can about the intruder (e.g., IPaddress).
- Temporarily or permanently block the intruder's IP address from the network, if possible. Monitor the IP address or user for future attemptsto access the network.
- Assess whether to reclassify the incident.

Additional Step for Severity 2 Incidents: Warn

- Ask 24 Exchange's Internet Service Provider (ISP) to collect anyinformation possible related to the possible attack.
- Determine how the attacker accessed the network.
- Notify and keep management updated about the incident.
- Assess whether to reclassify the incident.

Additional Steps for Severity 1 Incidents

- *Eradicate:* Eliminate the intruder's means of access and any related vulnerabilities.
- *Recover:* Based on the intruder's actions, what are the potential risks oractual damage? Mitigate that damage as much as possible. For example, if files have been deleted or modified, replace them with files from the physical or cloud backups. If network passwords have been compromised, require all employees to change their passwords on theirnext login and consider a more robust password policy / mandatory password manager use[4]. As well, you may use the Disaster Recovery/ Business Continuity procedures.
- *Perform Root Cause Analysis:* How did the hacker/intruder access the network? What techniques could prevent similar attacks in the future?

Code Errors Deployed to Client

If a software bug is deployed to clients, it's important to make sure that codeerror won't cause any security incidents. Consequences could be: data loss,system outages, features failing to work, or interruptions in functionality.

Severity 3 Incidents: Contain and Monitor

- Assess the code error to see whether or not it could cause a securityincident or serious problem for the client.
- If the code error would not cause a security incident according to the assessment, fix the error and deploy the update when possible.
- If the code error might case a security incident/breach, upgrade theincident to a Severity 2 immediately.

Severity 2 Incidents: Contain, Monitor, & Warn

- If possible, revert the client's software to an earlier, secure, version.
- Rewrite and test the code.

[4] Two factor authentication (2FA) is currently in the process of being implemented.

- Deploy the new updates as soon as possible.
- Notify the clients using the deployed code and see whether any problems have occurred because of it. If any incident has occurred,reclassify the incident as Severity 1.
- Notify and keep 24 Exchange management updated about the incident.

Additional Steps for Severity 1 Incidents

- *Eradicate:* Deploy the updated, tested code.
- *Recover:* Work with the involved companies to fix any problems thatthe code caused (e.g., network outages, security breaches).
- *Perform Root Cause Analysis:* What was the origin of the code error? Why wasn't the error discovered in the testing process? How should thetesting process be changed given this experience?

Social Engineering

Severity 3: Contain and Monitor

- Get a copy of the possible phishing email/text message.
- Use a quarantined or isolated computer/network to test any links and attachments for malicious intent.
- Add the sender's email to company-wide spam filters.
- Blacklist the domain of suspicious links.

Additional Step for Severity 2 Incidents: Warn

- For phishing attempts, send company-wide email with screen shots ofthe email and a reminder of the signs of phishing.
- For spear phishing and whaling attempts, contact the management involved as well as their direct reports to warn them that they shouldverify requests in person where possible.
- Notify and keep 24 Exchange management updated about the incident.
- Assess whether to reclassify the incident as Severity 1.

Additional Steps for Severity 1 Incidents

- *Eradicate:* Require everyone involved to change their passwordsaccording to the Password Policy. Make sure they have unique passwords.
- *Recover:* If information has been lost, use the available processes torecover.
- *Perform Root Cause Analysis:* How did the social engineer trick the involved parties? How can you improve security awareness training toprevent this type of attack? Did a whaling attack involve confidential orsensitive information about the client, company or an executive? If so,how might the attacker have accessed that information? Is a company email account/password compromised? Review the password policy to ensure it's robust enough, and consider mandating password managersand/or two-factor authentication.

Fraud

Severity 3: Contain and Monitor

- Collect as much information you can about accounting discrepanciesand store that information in multiple locations (online and offline).
- Check for alternates to fraud: e.g., typos, software error
- If you can't rule out fraud, escalate to a Severity 2 Incident.

Additional Step for Severity 2 Incidents: Warn

- Determine who accessed the accounts or accounting files. Did everyonewith access have permission? If it appears so, increase this to a Severity1 incident (internal).
- If an external party appears responsible, try to determine the means ofaccess.
  - For a network attacker, follow the "Network Attack" procedures.
  - If there was a physical security breach, follow the "Physical Security"procedures.
- Notify and keep management updated about the incident, and considerwhether law enforcement or a forensic accountant should be involved.
- Assess whether you should reclassify the incident as Severity 1.

Additional Steps for Severity 1 Incidents

- *Eradicate:* Destroy all unneeded data (physical or electronic).

- *Recover:* If the data has been lost, use the available processes torecover.
- *Root Cause Analysis:* How can you improve awareness training to prevent this type of fraud in the future? How might the attacker haveaccessed that information? Is the data unrecoverable?

Contain and Limit the Exposure: More Details

Within 24 hours of a security compromise, thoroughly investigate any suspected or confirmed loss/theft of account information. In this process, youshould:

- Keep a detailed log of who does what actions throughout the process.Make sure you save this log and any other evidence (e.g., electronic, video).
- Preferably, keep copies in multiple locations and multipleforms.
- Follow best practices for chain of custody throughout the investigation.Keep a clear paper trail of who has the evidence and/or equipment at alltimes.
- Work with legal and management to identify an appropriate forensicspecialist for any required forensic investigations.
- If a system is compromised, make sure no one accesses or changes it.
- If a machine is compromised, make sure no one turns it off or closesany applications. Instead, isolate or quarantine the system from thenetwork.
- If a wireless network is involved in the incident, change SSID on anyaccess points and other machines that may be using this connection.Exception: any systems believed to be compromised

Perform a Root Cause Analysis & Debrief Affected Parties: More Details

Within a week of the incident, meet as a team with the affected parties toperform a root cause analysis. In this meeting:

- Review the investigation's results
- Determine what allowed the security incident to happen (i.e., the rootcause)
- Evaluate the incident response plan's effectiveness
- Review any related security controls to determine whether they are appropriate

- Use what you've learned to improve and update any relevant securitymeasures, controls policies, and plans

If the investigation determines that an employee is a malicious actor, management and Human Resources should work together to address the issueappropriately, following all relevant policies and employment law.

Educate and Test All Employees

To make sure everyone is prepared for security incidents, Chief Information Security Officer to provide incident response training regularly.

Chief Information Security Officer will plan a test incident at least once ayear to ensure that everyone can implement the security incident plan andthat the current plan is effective.[5]

All 24 Exchange employees, consultants, advisors and directors are notified by email of this Policy and its location.

IT Roadmap

The IT Roadmap represents a forward-looking roadmap for enhancements to the Information Security and Cybersecurity Programs for the next 2-3 years.

1. **ISO 27001 Certification**
2. **Security Testing Program Update: internal/external vulnerability scanning**
3. **Use Active Directory to manage access control**
4. **Improve permission management and separation of database application users**
5. **Use Jira for change management, request management for access/email, incident management etc.**
6. **Create a full list of what we backup currently, identify what more we need to backup and for how long and address gaps.**
7. **Implement 2FA**
8. **Improve monitoring system for hardware and software issues**
9. **Complete email transition from GoDaddy to Microsoft with security features**

[5] To be implemented in 2023.