Information Security Statement

October 2018

Itiviti Group AB

Table of Content

Change control

VERSION	DATE	Change summary	NAME
1.0.0	28/09/2016	Initial Release	O. McKenzie
1.0.1	26/10/2016	Minor wording changes	D. Vagner
1.1.0	26/10/2016	Approved version	All approvers
1.2.0	27/04/2017	Annual review and update	O. McKenzie
1.3.0	01/05/2018	Annual review and update	O. McKenzie
1.3.1	04/10/2018	Change to represent Itiviti	O. McKenzie P. Gisseman

Approvals

APPROVER	TITLE
E. Ryst	CIO
J. Albert	CLO

Overview

Itiviti Group (“Itiviti”) has endeavored to design and implement an Information Technology infrastructure and Information Security and Risk Management program that is generally aligned with industry best practices and standards. The infrastructure security controls and associated information security processes were developed to protect confidential information while making it available in all appropriate circumstances. A summary of such policies, controls, and associated processes is set forth below. From time to time, Itiviti may change these policies, controls and associated processes. Itiviti shall not be under any obligation to notify any client of any such change.

Purpose

The purpose of the Information Security Statement is to provide clients, prospective clients, and vendors with an overview of Itiviti Information Security practices Information is a very significant business asset for Itiviti and therefore needs to be protected. Information exists in many different forms. It can be provided verbally, be written on paper, be stored electronically, be on film, or transmitted digitally. Irrespective of the way information may exist, be stored or transmitted, it must be protected in an appropriate manner.

Itiviti requires information security to mitigate security risks to information assets. It is critical to protecting the company’s proprietary and sensitive information to maintain a competitive advantage in the marketplace, to ensure profitability, and to secure and maintain customer and partner trust and confidence.
Security threats originate at a wide variety of sources, including computer-assisted fraud, industrial espionage, sabotage, vandalism, and natural disasters. Computer viruses, unethical hacking, and denial of service attacks are examples of threats encountered while operating over the Internet. These types of threats are becoming increasingly more common, more ambitious and more
sophisticated.

Therefore, Itiviti’s overall information security objectives are as follows:

- To have well-functioning information procedures within its operations and activities
- To proactively identify and mitigate security risks to the organization's information assets
- To ensure customer trust by providing assurance about the company’s products and services
- To ensure the company's long-term growth, competitiveness, and survival.

What is Information Security?

According to ISO 27001:2013 detailing the international standard's vocabulary, information security is "[the] preservation of confidentiality, integrity, and availability of information", thus outlining three general objectives for protecting information. These objectives are defined below.

Confidentiality

Confidentiality is achieved by ensuring that information is accessible only to those authorized to have access. If an unauthorized person, computer system, process, or other entity gains access to information (either voluntarily or involuntarily), confidentiality is compromised.

Integrity

Integrity is achieved by safeguarding the accuracy and completeness of information and processing methods. Integrity can be compromised through malicious altering (e.g. attackers manipulating details of financial transactions), accidental altering (e.g. transmission errors, a hard disk crash), or programming errors resulting in data inconsistencies.

Availability

Availability is achieved by ensuring that authorized users, systems and processes have access to
information and associated assets when required.

Information Security Statement

Information Security, Risk, & Governance

In order to meet overall risk management objectives, each business function within Itiviti is required to identify, assess, measure and control its operational risk in line with the Itiviti policies. Itiviti continuously assesses the risk and evaluates the need for protective measures. The head of each business function is responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the Itiviti policies.

Itiviti maintains an Information Security, Risk & Governance team to oversee its information security program. The team is headed by Itiviti's Chief Infrastructure Officer. The team is responsible for:

- Security Risks & Compliance Governance
- Security Standards & Architecture
- IT e-Discovery & Investigations
- Vulnerability Assessment & Analysis

Members of the team hold various industry security and audit based certifications (e.g., CISSP, CISSAP, and CISM).

Information Security Policy

Itiviti maintains a comprehensive information security program which includes policies, standards, and procedures. This program is based on industry guidelines and best practices including ISO/IEC 27001:2013, National Institute of Standards and Technology (NIST) Cybersecurity Security Framework, and the BITS Financial Institution Shared Assessments Program. The program provides a framework to ensure the security controls used to protect customer data are effective and operating optimally.

Company leaders meet on a regular basis to consider strategic and tactical direction for the information security policies, standards, and procedures.

Itiviti Information Security Policies are drafted with input from internal information security resources and are based upon industry best practices. The drafts are reviewed and approved by the Operational Leadership and the Executive Leadership Teams. Once approved, the policies are published on the company's intranet and communicated to all personnel.

Awareness and Training

Itiviti has implemented a training and awareness program for all employees. The program covers all information security related topics included in the company's policies, confidentiality agreements, and information protection standards. All Itiviti personnel are required to complete information security awareness training during the new hire onboarding process and are re-

trained annually. All individuals who have access to Itiviti's intranet are presented with an information security policy awareness statement once each year.

All Itiviti personnel are also required to complete a privacy, ethics, and anti-bribery training course. Itiviti constantly enhances employees awareness of security risks and issues through policies and processes adjustments, newsletters, and security testing.

Disaster Recovery / Business Continuity Management

DR / BCP

While the goal of the overall security program is to reduce the likelihood of a disruption, Itiviti has developed and implemented a Disaster Recovery and Business Continuity Program that enables the recovery of company's infrastructure so that the end-to-end business process can continue should a disruption occur. Itiviti's program includes the following basic activities:

- Prioritizing the activities to be recovered by conducting a Business Impact Analysis
- Performing a risk assessment for each of the IT services to identify the assets, threats, vulnerabilities
- and countermeasures for each IT service
- Evaluating the options for recovery; producing a contingency plan; and testing, reviewing, and revising
- that contingency plan on a regular basis.

These activities are documented and referenced in Itiviti's Business Continuity Plans (BCP). The BCP contains emergency response procedures that go into effect within a reasonable period of time following the occurrence of a disaster or other unplanned interruption, including assessing the wellbeing of personnel, providing for the continuity of essential business functions, and utilizing recovery procedures for critical business processes.

In summary, Itiviti has a comprehensive Disaster Recovery / Business Continuity Program that provides emergency response procedures for the continuity of essential business functions, and recovery procedures for critical business processes within a reasonable period of time following the occurrence of a disaster or other unplanned interruptions.

Pandemic Planning

As described above, Itiviti takes disaster and contingency planning very seriously, including planning for various pandemics. The planning undertaken by Itiviti to address a possible pandemic scenario involves endeavoring to maintain the continuity of essential business functions. Current plans address issues such as technology, communications, travel, resource allocation, and alternate work sites. Itiviti's ongoing planning encompasses the following areas:

- Communications
- Client Service
- Office Services/Facilities
- Human Resources and Travel

- Procurement and Vendor relationship
- Information Technology
- Finance
- Risk Management

The following is a brief summary of some specific activities completed or currently underway:

- Specific action steps and activities were identified in the various areas listed above, and more detailed action plans are being developed.
- Itiviti initiated pandemic awareness education for its personnel, including training for local, regional, and global leadership teams.
- Itiviti monitors for possible pandemic events in all countries where Itiviti maintains an office.

Itiviti anticipates that the planning process and its activities will continue to evolve. Itiviti will continue to monitor information and news sources regarding current threats, including the progression of human infections, and, as the circumstances and facts warrant, Itiviti expects to adjust its plans as appropriate. Accordingly, there will not
be a “final” plan, but rather a plan that can be adjusted to the extent warranted. Itiviti has teams in place that are ready to respond to such threats and to implement plans should the situation warrant.

Limits of BCP and Pandemic Planning

Due to the significant uncertainties associated with a possible a pandemic or other disaster, Itiviti can make no representations or warranties, nor can Itiviti provide any assurances, that its plans will be adequate to respond to all possible consequences, or that the plans of any third parties to deal with a possible pandemic or other disasters will be sufficient to address all situations or problems that might arise during a pandemic or other disaster. Itiviti’s objective is to prepare for a possible pandemic or other disaster based on the information and data that it has at the time and to possibly modify those plans as it believes conditions or facts may warrant.

Every organization needs to develop its own preparedness plan based on its specific circumstances, business functions, and operational factors. Consequently, a plan developed for one function or business cannot be expected to address the potential issues that may be faced by another business enterprise. Business continuity plans, policies, and documentation contain information about Itiviti is proprietary and confidential.

Human Resources Security

Upon hire, all personnel agrees to comply with Itiviti’s policies, including those relating to confidentiality and privacy. In addition, all Itiviti personnel is required to complete security awareness training during the new hire onboarding process.

Background Checks for U.S. Personnel

Itiviti generally requires that background investigations be conducted for all personnel at the time that they join Itiviti. Potential issues that are identified in the background investigations are reviewed to determine if they pose a risk to Itiviti, its personnel, or clients. The type of background investigation performed depends on whether the individual joining Itiviti is a partner, principal, or a regular employee. All background investigations of Itiviti's personnel in the U.S. currently include the following, at a minimum:

- SSN verification: confirms a valid number and that it belongs to the individual;
- Felony and misdemeanor conviction searches: searches for felony and misdemeanor convictions are performed for the last five years at the following levels: federal, state (where available and reasonable) and counties of residence, work, and school;
- Education confirmation: all education beyond high school confirmed;
- Employment confirmation: all professional employment in the last five years is confirmed -- minimum of dates of employment and position held, and an attempt is made to obtain rehire status, a reason for leaving, and salary; and
- SEC search, OFAC search (suspected drug dealers, money launderers, terrorists), GSA search (barred from working on or receiving government contracts), FDA search (barred from working at or being associated with pharmaceutical companies), FBI Most Wanted search, EU Terrorist Watch List search, and Interpol Watch List search

Background checks for EMEA Personnel

The type of background investigation performed depends on whether the individual joining Itiviti is a partner, principal, or employee, and the level of the employee. All background investigations of Itiviti's personnel in the UK offices currently include the following, at a minimum:

- Education confirmation: Graduation and Post-Graduation, as applicable; and
- Employment Verification: Last 5 years of employment or last 3 employers, as relevant.

Background checks for Asia Pacific Personnel

The type of background investigation performed depends on whether the individual joining Itiviti is a partner, principal, or employee, and the level of the employee. All background investigations of Itiviti's personnel in the Asia Pacific UK offices currently include the following, at a minimum:

- Education confirmation: Graduation and Post-Graduation, as applicable; and
- Employment Verification: Last 5 years of employment or last 3 employers, as relevant.

Physical and Environmental Security

Only authorized personnel with an Itiviti electronic badge are granted access to Itiviti's facilities. Itiviti data centers are further restricted to only those personnel with the need to access restricted areas. Procedures exist for controlling visitor access and maintaining a detailed log

of all visitors to the computing facility. Data centers have at least the following physical protection measures: security guards, man-trap doors to be electronically opened by an authorized electronic badge, video cameras, and sign-in and sign-out sheets.

The electricity, water, and temperature controls are all pre-approved for use by the facilities administrators. Each utility has a control in place to monitor its usage and to notify an administrator in case of failure. Automatic emergency lighting is installed in areas necessary to maintain personnel safety.

Emergency exits are located in various places in the facilities. Automatic fire suppression systems are installed to protect the data centers and offices. Master water shut-off valves are present. Temperature and humidity controls are implemented to protect against temperature fluctuations in all areas of the facilities containing IT equipment.

Systems and Data Security

Systems and Communications Protection

An intrusion detection/prevention system (“IPS/IDS”) is employed at the point of entry to the Itiviti network environment. The logs for the IPS/IDS, firewall, and VPN are sent to a log aggregator. Access control lists are placed on firewalls controlling the inbound and outbound flow of traffic. Inbound traffic is denied by protocol unless approved. DMZ and trusted zones are used to segment traffic to areas that are protected in accordance with the accepted risk.

System and Information Integrity

Firewall, IPS/IDS, and VPN audit logs are sent to the log aggregator, which checks for abnormal activity and anomalous behavior that would trigger an information security review. Hardware and software checks are done by automated tools with identified alert levels that trigger a notification to the system administrators in case of a system flaw. Anti-virus is managed as part of an enterprise policy. Anti-virus is configured to scan external devices attached to the information system as well as email traffic.

Data Backup

Itiviti critical systems and/or data are either constantly replicated or regularly backed up to a remote site. If either of the processes is interrupted or failed for any reason, a notification is generated and sent to appropriate personnel. A reputable vendor is utilized for disposal of hardware assets. The vendor is subject to obligations of confidentiality, has security practices in place and uses a tracking application for all media it handles on Itiviti’s behalf, and stores the media in a secure, environmentally controlled facility (see data destruction below).

Data Confidentiality

Itiviti personnel receives training covering the proper handling of confidential information in accordance with Information Classification And Handling Policy. In the instances in which Itiviti

may transmit confidential information outside of the Itiviti environment, Itiviti requires its personnel to transmit confidential data in an encrypted format.

Data Encryption

Itiviti Internet mail gateways are configured to attempt to transmit all email in an encrypted manner if the recipient of the transmission can support such an encryption methodology. Opportunistic TLS is enabled on the Itiviti email gateways. If TLS is enabled on the recipient email gateway, the email will be encrypted between the gateways. Secure File Transfer Protocol (SFTP) is an available option for the transfer of client data. SFTP securely encrypts and compresses files during transmission.

Client's data in transit over public lines are subject to mandatory encryption (VPN).

Client's data in transit over private lines are subject to encryption upon client's request.

Data Destruction

Assets slated for disposal are to be disposed of within the region or country they were decommissioned in. Itiviti contracts an IT asset disposition service provider (ITAD). The first step in the process is performed by Itiviti staff, this is the basic data erase and formatting of all storage media. The asset is then transferred to the ITAD provider who will transport the asset to their facility for full wiping per DoD 5220.22-M and final disposal per e-Stewards® Enterprise recycling.

Vendor Assessment Process

Itiviti is currently in the process of implementing a Vendor Assessment Process that is designed to reduce vendor-related risk by:

- Building a repository of authorized and critical vendors
- Assessing the vendor security and financial stability posture
- Ensuring Itiviti's data is protected appropriately
- Tracking identified remediation of issues

Asset Management Process

Itiviti has a technology asset management process that follows approved processes for asset management. There are tools and controls in place that manage all hardware and software assets which are reviewed on an annual basis. Itiviti has policies and procedures in place to manage licensed software and deter unapproved software from being loaded. A software and hardware inventory system is maintained, which identifies hardware and software components used within the information systems.

Access Control

Users are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All access must be approved by the Itiviti data owner. All users must be authenticated using a unique user ID and a strong password prior to gaining access to the information system.

Vendor and contractor access are requested via a formal access and authorization process. Upon approval, the vendor user accounts are created in a controlled domain organizational unit giving access necessary to perform their defined duties only. Vendor and contractor access are granted on a temporary basis requiring regular renewal approval by the asset owner.

Remote access is provided via a VPN solution that integrates with a Multiple Factor Authentication system and supports account activity logging to Itiviti's logging/alerting infrastructure. Depending on the level and type of access required, the VPN solution provides a virtual session or web interface into the needed application(s).

Privileged user accounts to Itiviti IT systems are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, and web administration).

Information Systems Acquisition, Development, and Maintenance

Acquisition of System and Services

Itiviti does not acquire new systems or services without in-depth review to determine whether it meets guidelines in regards to security and other risks. Software installation requests are submitted for risk assessment and approval. The software is not implemented unless it meets Itiviti Information Technology Security standards. Change Control Board has to review any additions to be sure that it will not affect the security posture and/or stability of the environment.

Application Development

Itiviti development process follows secure software development best practices, which include formal design reviews by the Information Security Team, threat modeling, and completion of a risk assessment. Static code analysis tools are run as a part of the standard build and integration process, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts.
Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations.

Change Control

Itiviti applies a systematic approach to managing change so that changes to customer-impacting services are thoroughly reviewed, tested, approved, and well-communicated. The

Claimfox change management process is designed to avoid unintended service disruptions and to maintain the integrity of service to the customer.
Changes deployed into production environments are:

- **Reviewed:** Peer reviews of the technical aspects of a change are required.
- **Tested:** Changes being applied are tested to help ensure they will behave as expected and not adversely impact performance.
- **Approved:** All changes must be authorized in order to provide appropriate oversight and understanding of business impact.

Changes are typically pushed into production in a phased deployment starting with lowest impact areas. Deployments are tested on a single system and closely monitored so impacts can be evaluated. Rollback procedures are documented in the change ticket. When possible, changes are scheduled during regular change windows. Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

Maintenance

Itiviti Information Systems and Infrastructure teams perform software and hardware maintenance on Itiviti's environment servers. If a vendor involvement is required, the third party maintenance personnel must be approved prior to receiving access to the information systems. A log is maintained which documents the name, date, length of time, justification, and escort name for each maintenance personnel who is granted access to the information system(s).

Information Security Incident Management

Itiviti incident response process follows Itiviti Incident Response Policy and brings together the appropriate subject matter experts from various disciplines to address each specific incident. The Security Incident Response Procedures ("Procedures") describe how various types of incidents are handled and identify key resources and communications that will take place based on various incident types.

The Procedures identify to whom suspected incidents should be reported and describe the escalation path from the entry point in the process. Security awareness training is in place to make Itiviti personnel aware of their responsibilities concerning security incidents. Each incident is logged and the relevant facts are captured. When necessary, data related to the incident is maintained in a forensically sound manner and appropriate chain of custody is documented.

The incident response team has a variety of tools available to assist them in the analysis of incidents. These include standard security tools from software and hardware providers as well as commercial forensic tools specifically targeted for such matters.

The Procedures are executed periodically so the teams remain prepared for response should the need arise. At the completion of each significant incident, a post-incident review is

conducted to identify any areas for improvement as well as areas that went well. These findings are used to adjust and improve the Procedures.

Compliance

System Audit and Accountability

Audit records are created the following services:

- intrusion detection and prevention services;
- remote access services, web proxy services;
- domain authentication;
- firewall events, VPN access;
- anti-virus services; and
- application logs.

Audit records are maintained to support analysis and investigations of past and current events. Logs are maintained based on file size and the retention time may vary but they are typically archived for at least 90 days. Logs are also maintained based on regulatory requirements.

Audit record content includes: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) unique user/subject identity; and (v) the outcome (success or failure) of the event.

System Audits

Internal security control reviews are performed at least annually by an independent 3rd party security firm. Audits are performed on various aspects of systems and include reviewing, standards, processes, and policies.

Application Configuration Management

Software baseline configurations are created in accordance with Itiviti policies and standards. The software is tested against the baseline requirements prior to being placed in the production environment. Continued monitoring is conducted while in operation.

System Monitoring, Logging, and Alerting

Itiviti monitors servers, workstations and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in Itiviti's production network are logged.

Itiviti's Security Team collects and stores production logs for analysis. Logs are stored in a separate network. Access to this network is restricted to members of the Security Team. Logs are protected from modification and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. Alerts are examined and resolved based on documented priorities.

Records Management

Itiviti maintains and retains records in accordance with applicable legal and regulatory requirements and professional standards.

Related Standards, Policies, and Processes

Itiviti-Security_Policy
Itiviti-Information_Classification_And_Handling_Policy
Itiviti-Asset_Management_Policy
Itiviti-Acceptable_Encryption_Policy
Itiviti-Incident_Response_Policy
Itiviti-Information Systems BCP
Itiviti-Change_Management_Process

About Itiviti

Itiviti is a market-leading global provider of multi-asset trading technology and financial infrastructure solutions for buy-side and sell-side market participants, including NYFIX, one of the industry's largest FIX-based trading communities.

Serving more than 1,900 clients worldwide, we provide consistent, reliable access to the most up-to-date and innovative order routing, connectivity and trading solutions available. Top-tier trading firms, banks, brokers, exchanges and institutional investors rely on our technology, solutions and expertise to streamline their daily operations, connect to their desired markets, and trade when and where they want. All while being able to comply with global regulation.
With global offices in 18 locations covering all major financial centers the merger of Itiviti and ULLINK in March 2018 created a full service technology and infrastructure provider, covering all asset classes, geographies and regulatory landscapes.

For more information, please visit www.itiviti.com or www.ullink.com.

Itiviti is owned by Nordic Capital Fund VII.