SECURITY WHITEPAPER

Itential Platform

Itential - Public

What is the Itential Platform? 2
Executive Summary 2
Our Product 2
Data We Collect 2
Our Cybersecurity Program 3
Our People 3
Securing Our Environment 4
Our Third Parties 5
Itential Customer Commitments and Compliance 6
Shared Security Responsibility 6
Customer Responsibilities 6
Product Security Features 6
Itential Responsibilities 6
Itential Information Security Objectives 7
Confidentiality 7
Integrity 7
Availability 7
Appendix A 8
Information Security Policy and Organization 8
Risk Management 8
Asset Management Policy 9
Access Control Policy 11
Cryptography Policy 11
Physical and Environmental Policy 12
Change Management Policy 13
Vulnerability Management Policy 13
Incident Management Policy 14
Business Continuity Planning Policy 14
Compliance Policy 15
Endpoint Management Policy 15
Personnel Security Policy 15

WHAT IS THE ITENTIAL PLATFORM?

The Itential Platform is a cloud-native network and enterprise automation and orchestration platform that enables automated configuration and compliance for hybrid, multi-cloud networks. Protecting the confidentiality, integrity, and availability of customer data is a top priority, and it is established and maintained in the design of Itential's systems. This white paper documents Itential's compliance, cybersecurity, and operational practices.

EXECUTIVE SUMMARY

Our Product

The Itential Platform is a SaaS, shared tenant product running in the AWS US East 2 (Ohio) region. Client data and accounts are logically separated within our systems through the use of account ID's and permissions. Clients have the ability to control authentication to the product via RBAC and GBAC functionality. Internally, Itential leverages authentication best practices for employees through the use of MFA.

High availability and low latency of the Itential platform is achieved through multi-AZ redundant architecture in AWS. Where applicable, Itential adheres to best practices as recommended by AWS when configuring our AWS environment. Information on AWS' certifications related to security and compliance can be found at this web address: https://aws.amazon.com/compliance/programs/

Data We Collect

Itential is not a platform for sensitive data about individuals. Itential processes and stores names, email addresses, and IP addresses of Itential users. IP addresses of Itential website viewers are tracked via internal analytic tools; however, IP addresses are not used to identify users. While Itential collects IP address data, this data is for internal use only.

For more information, please review the Itential Privacy Policy.

OUR CYBERSECURITY PROGRAM

Itential's information security policies are approved by management, published, and communicated to employees and relevant external parties. These policies, including their related standards, guidelines, procedures, and controls, support the management of information risk and support the confidentiality, integrity, and availability of the product and data. Information security policies in place include the following:

- Information Security Policy and Organization
- Risk Management Policy
- Asset Management Policy
- Access Control Policy
- Cryptography Policy
- Physical and Environmental Policy
- Change Management Policy
- Vulnerability Management Policy
- Incident Management Policy
- Business Continuity Planning Policy
- Compliance Policy
- Endpoint Management Policy

Refer to Appendix A for summarization of the aforementioned policies.

Our People

We perform background checks on all employees. All employees must sign an NDA prior to employment and annual security and privacy awareness training is provided. Access to Itential systems is provisioned based on the least-privilege principle when an employee is hired, an existing employee's role is changed, and removed upon termination. Prior to termination, HR compiles a list of access that must be revoked and works with department managers to ensure the list is comprehensive. Immediately upon termination, HR and system access managers revoke access to all listed systems.

Itential is headquartered in Atlanta, Georgia, and maintains a global presence. Our engineering organization has a limited team of full-time employees who are responsible for maintaining access to hosted systems containing Client data.

Securing Our Environment

We perform external network vulnerability scans through a third party on at least an annual basis. An annual penetration test is also performed by a third party. Additionally, we subscribe to vulnerability updates for all of our systems and automate vulnerability detection through our secure development processes. Any time vulnerabilities are identified, be it through external feeds or through vulnerability/penetration testing, they are prioritized based upon risk. When a remediation plan exists, vulnerabilities are prioritized accordingly.

Itential transmits data over the public Internet using TLS 1.2 with SHA-256 certificates. AWS VPCs are utilized to protect systems by closing all ports except those required to serve Internet traffic. Additionally, tools are in place to monitor our internal network for intrusions.

Our servers are built upon Hardened AWS Amazon Machine Images (AMIs). All changes to the Itential application go through the full secure SDLC, including peer review, functional and automated testing, and release testing/approval.

Daily backups and point-in-time restorations are configured

The email address vulnerabilities@itential.com is available to report security related incidents and is monitored 24x7.

Our Third Parties

Itential uses various vendors in the delivery of services to customers and to support the Itential application. Below is a non-exhaustive list of current, relevant third parties and sub-processors.

Vendor, System, or Application	Business Function / Description
Amazon Web Services (AWS)	Web hosting and services provider for functionality like Virtual Private Cloud, Virtual Private Gateway, S3, Elasticache, EKS, ECR, Cloudwatch, and Bottlerocket.
MongoDB Atlas	Cloud database service for Itential's native MongoDB database.
Microsoft O365	Subscription service offered by Microsoft for standard enterprise productivity software.
Gitlab	Web-based DevOps life cycle management tool with Gitrepository manager.
Jira	Customizable tool for agile software development; logs and tracks progress for bugs, tasks, features, and projects.
Slack	Web and desktop application for IRC-style persistent chat rooms, private groups, direct messaging, and notification automation.
Okta	Cloud software for identity and access management of internal Itential personnel.

ITENTIAL CUSTOMER COMMITMENTS AND COMPLIANCE

Itential does not own or house data subject to privacy regulation, however, Itential has implemented a robust information security program to offset possible threats, as well as controls that preserve information security objectives over confidentiality, integrity, and availability:

- Confidentiality: Information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity: Information is complete and accurate.
- Availability: Information is accessible and usable on demand by an authorized entity.

Itential receives its SOC 2 Type 2 audit report annually in October. The report is available upon request.

SHARED SECURITY RESPONSIBILITY

Customer Responsibilities

The Itential platform is not designed to house and protect individual's confidential information. As such, customers should ensure that all data is scrubbed of sensitive information (e.g., PII, ePHI) prior to uploading to the Itential Platform.

Product Security Features

Itential supports both password authentication and enterprise SSO using identity standard SAML integration.

Itential Responsibilities

We are honored that great companies trust us to automate their network operations. Our commitment is to continue to earn your trust through transparency, accountability, and by providing a reliable and secure platform. In the event of a breach or incident that affects you, we will notify you in a timely fashion.

Vulnerabilities can be reported at vulnerabilities@itential.com.

ITENTIAL INFORMATION SECURITY OBJECTIVES

Confidentiality

The infrastructure within AWS is designed to ensure confidentiality and privacy of user data stored and shared using the Itential application. Access to customer data is restricted through role-based security. Access to Itential source code, stored procedures, and associated items (e.g., designs, specifications verification, and validation plans) is strictly controlled. These access controls are in place to prevent the introduction of unauthorized functionality, avoid unintentional changes, and preserve the confidentiality of valuable intellectual property.

Itential's confidentiality requirements and commitments are communicated to third parties through contractual agreements. Legal counsel is responsible for drafting terms and conditions, as well as approving any changes to those terms. Itential is responsible for ensuring these contracts are in place for all third parties with access to the Itential application.

Integrity

To ensure the integrity of data on Itential's application, regular updating of corporate or hosted software, applications, and program libraries is performed by trained administrators and based on approval from appropriate management. All changes and upgrades to Itential systems are performed according to documented and approved Change Management policies and procedures. Access controls are in place throughout the Itential application, supporting infrastructure systems, AWS, and supporting software to prevent unauthorized changes to data and systems.

Availability

Scalable database systems are deployed across regional and zone-redundant storage systems via MongoDB Atlas. Each zone is geographically separated to avoid a single point of failure. Data is replicated to all zones in real time. Additionally, redundant backup copies are stored across multiple availability zones. Backup frequency and retention vary depending on the nature of the data and system. Itential performs tests of backups and restoration procedures for critical operations on at least an annual basis.

Enterprise-level Internet services are provided at Itential's headquarters. No critical systems infrastructure is housed or hosted at the Itential headquarters. In the event a disruption affected the headquarters, Itential as a Company, and the Itential application could continue functioning without interruption.

APPENDIX A

The purpose of this section is to provide a brief overview of Itential's security framework. Only key policies and procedures are covered in this section. All policies, not just those summarized here, are published on internal collaboration tools and accessible to all employees.

Information Security Policy and Organization

Itential has a documented and approved Information Security Policy that defines, on a high level, Itential's commitment to security. The policy also documents key personnel and their associated security responsibilities and a high-level summary of the policies and procedures in place to help establish and promote a security culture at Itential.

Itential has established a security committee. The security committee is responsible for oversight, review, and approval of all security related policies, audits, risk assessment approval and remediation, and the general approach of promoting a security culture at Itential.

Risk Management

Itential performs an internal risk assessment at least annually and upon significant changes to the environment (e.g., acquisition, merger or relocation, introduction of new regulatory requirements). The risk assessment process aligns with industry best practices frameworks and includes the following elements:

- Identifies, analyzes, and evaluates critical assets, threats, and vulnerabilities;
- Results in a formal risk assessment that includes mitigating controls, evaluation, and prioritization of those controls to determine if they reduce the overall risk exposure to Itential; and,
- Ensures that repeated information security risk assessments produce consistent, valid, and comparable results.

Risks are categorized, prioritized, and remediated based on the likelihood and impact of an effect on Itential's commitments. Identified risks are addressed through the information security risk treatment plan, and the results of treatment plans are retained. Risk treatment methodologies include the following:

- Risk Acceptance: Accept potential risk and continue operating.
- Risk Avoidance: Avoid risk by eliminating the risk cause and/or consequence.
- Risk Mitigation: Minimize risk by implementing preventive and detective controls.
- Risk Share/Transfer: Lower the risk by acknowledging the vulnerability and transferring the risk to a 3rd party (i.e., insurance) or share with another party.

Identified risks are assigned an owner who is responsible for approving the risk treatment plan and accept any residual risks.

Third Party Risk Management
Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain, including the execution of confidentiality agreements. The risk and security team vet new vendors and perform annual reviews, where necessary, of existing critical vendors.

Itential regularly monitors, reviews, and audits third party service delivery using a risk-based approach as follows against the Company's information security objectives:

- Determine criticality of identified third parties;
- Assess the impact of identified threats and vulnerabilities;
- Assess the likelihood of identified threats; and
- Determine the risk associated with the third party based upon criticality, threat impact, and likelihood.

Third party risk assessments are reviewed and updated if necessary, based on the results of monitoring. The frequency of evaluations depends on the risk to Itential's information security objectives and of noncompliance to Itential policy (e.g., enterprise strategy, information security policies, laws, and regulations).

The right to audit during contract negotiations is considered to determine if Itential will be allowed to perform compliance audits on the vendor's internal controls, if the vendor will provide self-assessment reports, or reports prepared by independent assessors (i.e., SOC 2 examinations).

Asset Management Policy

Assets such as hardware, software, are assigned an owner and classified. Patch levels are also tracked to ensure systems, applications, and tools are running appropriate operating system or software version. Asset inventories are periodically reviewed for completeness and accuracy.

Ownership of Assets
Critical assets (or groups of assets) maintained in the inventory are assigned ownership. The asset owner is responsible for the proper management of an asset over the asset lifecycle. The asset owner:

- Ensures that assets are inventoried;

- Defines and reviews access restrictions and classifications to important assets, taking into account applicable access control policies; and,
- Ensures proper handling when the asset is deleted or destroyed.

Acceptable Use of Assets

Rules for the acceptable use of information and assets associated with information and information processing are identified, documented, implemented, and made available to all users. Employees are required to review and acknowledge the employee handbook, which includes rules for acceptable use of hardware, software, and data.

Return of Assets

The termination process is formalized to include returning all previously issued physical and electronic assets owned by or entrusted to Itential. All employees and third-party users are required to return all organizational assets in their possession upon termination of their employment, contract, or agreement. In cases where a user uses their own personal equipment (e.g., smartphone), procedures are followed to ensure that all relevant information is transferred to Itential and securely erased from the equipment, when feasible.

Access Control Policy

Itential uses the least-privilege access control methodology when granting user access to systems, tools, and infrastructure components. An access control policy is documented and followed by the Itential personnel responsible for granting and revoking access. Access, both internal and external, is reviewed regularly by department managers and security personnel. New, modified, or removed access is always documented and approved.

Itential system configurations are used to enforce password requirements according to industry-standard password parameters. Key components of the Itential Password Policy require that passwords and systems:

- Be stored in an approved password manager;
- Adhere to minimum character length specifications;
- Adhere to minimum character type specifications;
- Enable multi-factor authentication for all non-console, administrative access into IT assets that store sensitive or confidential data;
- Enable multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) if technologically feasible;

Cryptography Policy

Procedures defining the use of cryptographic controls for protection of information are in place and consider:

- The management approach towards the use of cryptographic controls across Itential (e.g., corporate and production environments), including the general principles under which business information should be protected with encryption;
- Based on a risk assessment, the required level of protection – taking into account the type, strength, and quality of the encryption algorithm required;
- Regulations or other restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of transborder flow of encrypted information.

Physical and Environmental Policy

Itential has implemented policies and procedures to prevent unauthorized physical access, damage, and interference to Itential information and information processing facilities. The infrastructure systems that support the Itential application are housed in AWS data centers. AWS is responsible for the physical and environmental security controls at such data centers. Itential reviews these controls on at least an annual basis. Physical and environmental security controls at AWS include the following:

- Uninterruptible Power Supplies (UPS) and generators are in place to provide backup power in case of service interruption;
- Fault tolerant data centers that are designed to anticipate and tolerate failure while maintaining service levels. This includes electrical power systems that are fully redundant;
- 24/7 monitoring of both physical and environmental security control mechanisms;
- Closed Circuit Television Camera (CCTV) recording of all physical access points to server rooms;
- Fire detection and suppression mechanisms including smoke detection sensors;
- Mechanisms to control climate and maintain appropriate operating temperature for physical equipment including servers; and,
- Regular maintenance of physical and environmental security systems and hardware.

Access to the Itential office facility is restricted to employees and authorized third parties via keycards. Individual physical access to sensitive areas (i.e., networking closets) is restricted via keycard access and monitored by video cameras. All visitors must sign in at the front desk and be escorted by an Itential employee at all times.

Physical access to Itential facilities is revoked immediately upon termination through notification to building management, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

Change Management Policy

Itential has formal and documented change management policies, procedures, and controls to prevent unauthorized changes to systems, tools, and infrastructure elements. All changes are documented in Itential's ticketing system and follow workflows that include requirements for testing, approvals, and segregation of duties.

The secure development life cycle (SDLC) consists of 5 basic stages: planning, implementation, review, testing and release. A risk assessment is performed during the planning stage. Mitigation and decisions on acceptable risk are determined prior to the implementation stage. Upon completion of implementation, a separate engineer performs a review of the changes including procedures to ensure the changes adhere to OWASP best practices.

All planned changes are reviewed prior to implementation to ensure they accomplish the acceptance criteria of the story. After peer review, changes undergo UX and functional testing as appropriate. Prior to release, the appropriate Software Development Manager reviews the changes and approves the release.

Itential uses manual code review based upon OWASP best practices and run the code through an automated linter and associated automated pipeline tasks.

Scheduled maintenance windows are communicated in advance via Customer Success Managers and also through the in-application notifications.

Itential does not develop customizations of its offerings. All customers received the same software and functionality.

Vulnerability Management Policy

Itential contracts with a third-party security firm to perform penetration tests on at least an annual basis. In addition, vulnerability scans are performed on product code repositories. Issues identified during the scans and tests are documented, tracked, and resolved according to Itential’s incident and risk management policies and procedures.

Procedures are in place to ensure the latest patches are deployed as they become available. Patches are applied according to Itential's change and vulnerability management policies using risk-based approach of patching.

Incident Management Policy

Incident management policies and procedures are in place that provide guidance on incident prevention and incident response.

Incident Detection & Prevention

Logging and alerting are configured in the Itential environment to capture actions in the Itential network and alert based on configured thresholds. The security and incident response teams are notified of alerts when triggered via email and remediates identified issues per policy. Itential systems are configured with appropriate prevention systems based on risk profile and threat modeling.

Incident Response Plan

The incident response plan consists of six phases:

- Preparation: Incident response team members are identified and tasked with identifying the “knowns” and “unknowns” surrounding the incident.
- Identification: More details are identified regarding the incident. This phase includes implementing monitoring and alerting tools to notify Itential of any potential incident.
- Containment: Focuses on methods that may be used to minimize damage to the business.
- Eradication: Once contained, the incident is managed based on the severity categorization designated in the identification phase.
- Recovery: Focuses on getting the system back to the original state.
- Lessons Learned: The goal of this stage is to verify that the incident is closed out properly and that all required actions have been taken to properly contain, eradicate and recover from the incident. This stage also includes implementing new procedures, policies, and/or solutions to prevent a similar incident from recurring in the future.

Business Continuity Planning Policy

Itential has a formal Business Continuity and Disaster Recovery (BC/DR) Plan in place to help ensure continuing service performance. The plan is tested at least annually, including a test restoration of backup data. Test results are documented, reviewed, retained, and mitigating measures are enacted, when necessary, as a result of the tests. The plan is also reviewed and approved on an annual basis.

Compliance Policy

Itential's information security policy is in place to avoid breaches of legal, statutory, regulatory, and contractual obligations related to information security and security requirements.

All applicable legislative statutory, regulatory, contractual requirements, both domestically and internationally, and the organization's approach to meet these requirements are explicitly identified, documented, and kept up to date for each business activity, information system, and the organization as a whole.

Acceptable use policy, asset registers, and asset disposal policies are implemented to ensure compliance with applicable legislative, regulatory, and contractual requirements related to intellectual property rights, including software or document copyrights, design rights, trademarks, patents, and source code licenses.

In addition, managers regularly review the compliance of information processes and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

Endpoint Management Policy

All devices are configured with endpoint management software that provides the following protections, consistent with the Asset Management and Personnel Security policies, as well as acceptable use policies:

- Full-disk encryption;
- Inactivity lockout; and,
- Anti-malware software.

Personnel Security Policy

Itential screens all associates prior to employment, which includes a background investigation. Issues identified during the background check process are resolved prior to employment and gaining access to Itential systems.

Employees are required to review and acknowledge the Information Security Policy, employee handbook, confidentiality and non-disclosure agreements, and the acceptable use policy upon hire. If these documents change, employees are required to review and re-acknowledge each document.

All Itential associates are required to undergo initial security awareness training upon hire and during the on-boarding process. In addition, active employees must undergo additional, role-based security training on at least an annual basis. Trainings are tailored to each role to help ensure Itential associates have the requisite training and knowledge to perform their job responsibilities.