

TripActions

Information Security Policy

V_1.7

Document Control

S. No.	Type of Information	Document Data
1	Document Title	Information Security Policy
2	Document Code	TA_POL_ISP
3	Date of Release	2018-05-18
4	Document Version No.	1.6.1
5	Document Owner	oleg@tripactions.com
6	Document Author(s)	oleg@tripactions.com

Document Approvers

S. No.	Approver Name	Approver Designation	Approver Email ID
1	Oleg Gusakov	CSO	oleg@tripactions.com

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
1.7	2019-06-27	Miscellaneous clean up	2019-06-17
1.6.1	2019-03-04	Removed content which overlapped separate, more detailed policies and procedures, including Access Control, Patch Mgmt, Incident Mgmt, etc.	2019-03-08
1.6	2019-01-25	1.5 - fixed typo in the reporting structure 4.3 - clarified exception for sharing keys with 3 rd parties 8.3 – removed antivirus exceptions 10.3 – clarified emergency change process 12.3 – added definition of internal info 14.3 – added OSS approval process	

1.5	2018-05-18	Added deletion of credit cards and account PII obfuscation - without activity in 3 years	2018-05-18
1.4	2018-03-08	Added, Change Management, Cryptography, SDLC, Incident Management policy	2018-03-30
1.3	2017-08-01	Updated address	2017-08-01
1.2	2017-06-29	Added data retention policy	2017-07-31
1.1	2016-06-01	Updated password policy	2016-06-19
1.0	2016-01-01	Initial	2016-01-01

Contents

- 1. INTRODUCTION..... 5
 - 1.1. Purpose..... 5
 - 1.2. Scope 5
 - 1.3. Responsibilities..... 5
 - 1.4. General Policy Definitions 6
 - 1.5. Security Policy Enforcement..... 6
- 2. IT ASSETS POLICY 6
 - 2.1. Purpose..... 6
 - 2.2. Scope 6
 - 2.3. Policy Definitions 6
- 3. PASSWORD CONTROL POLICY..... 7
 - 3.1. Purpose..... 7
 - 3.2. Scope 7
 - 3.3. Policy Definitions 7
- 4. EMAIL POLICY..... 8
 - 4.1. Purpose..... 8
 - 4.2. Scope 8
 - 4.3. Policy Definitions 8
- 5. INTERNET POLICY 9
 - 5.1. Purpose..... 9
 - 5.2. Scope 9
 - 5.3. Policy Definitions 9
- 6. ANTIVIRUS POLICY 10
 - 6.1. Purpose..... 10
 - 6.2. Scope 10
 - 6.3. Policy Definitions 10
- 7. INFORMATION CLASSIFICATION POLICY 10
 - 7.1. Purpose..... 10
 - 7.2. Scope 10
 - 7.3. Policy Definitions 10
- 8. DATA RETENTION, ARCHIVING AND DELETION POLICY 11
 - 8.1. Purpose..... 11

- 8.2. Scope 11
- 8.3. Policy Definitions 11
- 9. INFORMATION SYSTEM ACQUISITION, DEVELOPMENT and MAINTENANCE POLICY 12
 - 9.1. Purpose..... 12
 - 9.2. Scope 12
 - 9.3. Policy Definitions 12
- 10. REMOTE ACCESS POLICY 13
 - 10.1. Purpose..... 13
 - 10.2. Scope 13
 - 10.3. Policy Definitions 13
- 11. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING 13
 - 11.1. Purpose..... 13
 - 11.2. Scope 13
 - 11.3. Policy Definitions 13
- 12. OUTSOURCING POLICY 14
 - 12.1. Purpose..... 14
 - 12.2. Scope 14
 - 12.3. Policy Definitions 14
- 13. ANNEX..... 14
 - 1.1. Glossary 14

1. INTRODUCTION

TripActions’ Information Security Management System (ISMS) consists of a set of policies, processes, and systems to manage risks to organizational data, with the objective of ensuring acceptable levels of information security risk.

This Information Security Policy states the types and levels of security over the information technology resources and capabilities that must be established and operated in order for those items to be considered secure.

The Terms Organization and TripActions will be used interchangeably below in this document.

1.1. Purpose

This Security Policy document defines the security requirements for the proper and secure use of the Information Technology services in the Organization. Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

1.2. Scope

This document applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

1.3. Responsibilities

Roles	Responsibilities
Chief Security Officer	<ul style="list-style-type: none"> ● Accountable for all aspects of the Organization’s information security. ● Responsible for the security of the platform infrastructure. ● Plan against security threats, vulnerabilities, and risks. ● Implement and maintain Information Security Policy documents. ● Ensure security training programs. ● Ensure platform infrastructure supports Security Policies. ● Respond to information security incidents. ● Help in disaster recovery plans
Head of Compliance	<ul style="list-style-type: none"> ● Responsible for compliance with technical regulations and standards, including PCI-DSS, GDPR, SOC 2, ISO 27001 et seq, and CCPA.
Information Owners	<ul style="list-style-type: none"> ● Help with the security requirements for their specific area. ● Determine the privileges and access rights to the resources within their areas.
IT Security Team	<ul style="list-style-type: none"> ● Implements and operates platform security. ● Implements the privileges and access rights to the resources. ● Supports Security Policies.
Users	<ul style="list-style-type: none"> ● Comply with Security Policies. ● Report any attempted security breaches.

1.4. General Policy Definitions

- Exceptions to the policies defined in any part of this document may only be authorized by the Chief Security Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
- All the IT services shall be used in compliance with the technical and security requirements defined in the design of the services.
- Infractions of the policies in this document may lead to disciplinary actions. In some serious cases they could even lead to prosecution.

1.5. Security Policy Enforcement

Employees are encouraged to and shall report any situation in which they reasonably believe another employee of the Organization may not be adhering to this policy or any other situation in which they reasonably believe this policy is not being observed. Such reports shall be made to the Chief Security Officer unless the report directly or indirectly involves the Chief Security Officer, in which case the employee may report the situation to the Chief Technology Officer.

The Organization's business depends on strict application of this Policy, and Organization reserves the right to enforce this policy by any means allowed by applicable law(s), including, but not limited to, disciplinary actions.

2. IT ASSETS POLICY

2.1. Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in the Organization.

2.2. Scope

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

2.3. Policy Definitions

- IT assets must only be used in connection with the business activities they are assigned and / or authorized.
- All the IT assets must be classified into one of the categories in the Organization's security categories; according to the current business function they are assigned to.
- Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.

- Active desktop and laptops must be secured/locked if left unattended. Whenever possible, this policy shall be automatically enforced.
- Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.
- All personnel interacting with the IT assets must have the proper training.
- Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
- Access to assets in the Organization location must be restricted and properly authorized, including those accessing remotely. Company's laptops and other equipment used at external location must be periodically checked and maintained.
- The IT Technical Teams and DevOps (for assets in the cloud) are solely responsible for maintaining and upgrading configurations. No other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software. Any exceptions to this rule should be requested via issue tracking system and approved by CSO.
- Special care must be taken for protecting laptops and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
- When travelling by plane, portable equipment like laptops must remain in possession of the user as hand luggage unless mandated differently by the airline / authorities.
- Whenever possible, encryption and erasing technologies shall be implemented in portable assets in case they were stolen.
- Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the Chief Security Officer.
- Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of a Security Team member. Assets storing sensitive information must be completely erased in the presence of Security Team member before disposing.

3. PASSWORD CONTROL POLICY

3.1. Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in the Organization.

3.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

3.3. Policy Definitions

- Any system that handles valuable information must be protected with a password-based access control system. The production environment and the Cardholder Data Environment must be protected by MFA.

- Every user must have a separate, private identity for accessing IT network services.
- Identities shall be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- Each identity must have a strong, private, alphanumeric password to be able to access any service. They shall be at least 8 characters long.
- Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.
- Password for some special identities will not expire. In those cases, password must be at least 15 characters long.
- Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two sets of credentials: one for administrative work and the other for common work.
- Sharing of passwords is forbidden. They shall not be revealed or exposed to public sight.
- Whenever a password is deemed compromised, it must be changed immediately.
- For critical applications, digital certificates and multiple factor authentication using smart cards shall be used whenever possible.
- Identities must be locked if password guessing is suspected on the account.

4. EMAIL POLICY

4.1. Purpose

The Email Policy section defines the requirements for the proper and secure use of electronic mail in the Organization.

4.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

4.3. Policy Definitions

All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the Organization. Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the Organization system resources and the productivity of the work is not affected.

- Use of the Organization resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the organization business is strictly forbidden.
- In no way may the email resources be used to reveal confidential or sensitive information from the Organization outside the authorized recipients for this information.
- Using the email resources of the organization for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
- Use of the organization email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the

associated account must be deactivated according to established procedures for the lifecycle of the accounts.

- Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriated.
- Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the Information Security Officer may approve the interception and disclosure of messages.
- Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities. Sharing of passwords is discouraged. Users shall not impersonate another user.
- Outbound messages from corporate users shall have approved signatures at the foot of the message.
- Attachments must be limited in size according to the specific procedures of the Organization. Whenever possible, restrictions shall be automatically enforced.
- Whenever possible, the use of Digital Rights technologies is encouraged for the protection of contents.
- Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
- Security incidents must be reported and handled as soon as possible according to the Incident Management processes. Users shall not try to respond by themselves to security attacks.
- Corporate mailboxes content shall be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management.

5. INTERNET POLICY

5.1. Purpose

The Internet Policy section defines the requirements for the proper and secure access to Internet.

5.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3. Policy Definitions

- The use of messenger type services is permitted for business purposes.
- Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged.
- Internet access is mainly for business purpose. Some limited personal navigation is permitted if in doing so there is no perceptible consumption of the organization system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
- Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.

- In accessing Internet, users must behave in a way compatible with the prestige of the organization. Attacks like denial of service, spam, phishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
- Internet traffic shall be monitored at firewalls. Any attack or abuse shall be promptly reported to the Chief Security Officer.
- Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

6. ANTIVIRUS POLICY

6.1. Purpose

The Antivirus Policy section defines the requirements for the proper implementation of antivirus and other forms of protection in the organization.

6.2. Scope

This policy applies to servers, workstations and equipment in the organization, including portable devices like laptops and PDA that may travel outside of the organization facilities. Some policies apply to external computers and devices accessing the resources of the organization.

6.3. Policy Definitions

- All computers and devices with access to the organization network must have an antivirus software installed, with real-time protection turned on.
 - Antivirus for Mac to be installed on Mac machines.
- All installed antivirus software must automatically update their virus definitions. They must be monitored to ensure successful updating is taken place.
- Visitor's computers and all computers that connect to the organization's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

7. INFORMATION CLASSIFICATION POLICY

7.1. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the organization information.

7.2. Scope

This policy applies to all the information created, owned or managed by the organization, including those stored in electronic or magnetic forms and those printed in paper.

7.3. Policy Definitions

- Information owners must ensure the security of their information and the systems that support it.

- Information Security Management is responsible for ensuring the confidentiality, integrity and availability of the organization's assets, information, data and IT services.
- Any breach must be reported immediately to the Chief Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
- Information in the organization is classified according to its security impact. The current categories are: **confidential**, **sensitive**, **shareable**, **public** and **private**.
- Information defined as **confidential** has the highest level of security. Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
- Information defined as **sensitive** must be handled by a greater number of persons. It is needed for the daily performing of jobs duties, but shall not be shared outside of the scope needed for the performing of the related function.
 - Documents marked as **internal** contain sensitive information scoped within the company
 - For business purpose Table Of Content (TOC) of the **internal** documents can be shared with 3rd parties in case it is requested in order to conduct business
- Information defined as **shareable** can be shared outside of the limits of the organization, for those clients, organizations, regulators, etc. who acquire or shall get access to it.
- Information defined as **public** can be shared as public records, e.g. content published in the company's public Web Site.
- Information deemed as **private** belongs to individuals who are responsible for the maintenance and backup.
- Information is classified jointly by the Chief Security Officer and the Information Owner.

8. DATA RETENTION, ARCHIVING AND DELETION POLICY

8.1. Purpose

The Data Retention, Archiving and Deletion Policy section defines the requirements for the proper and secure handling including archiving and deletion of sensitive customer data the organization may get access to as part of its business.

8.2. Scope

This policy applies to all Organization employees and subcontractors who have handle the sensitive customer information with or without actually accessing the data.

8.3. Policy Definitions

- Information owner shall ensure that data is destroyed after its life.
 - Credit Card without activity in the last 3 years shall be deleted from the platform
 - Customer accounts without activity in the last 3 years will be deactivated, their PII - obfuscated
- All archived media having confidential or sensitive information shall be securely destroyed.

- Information on storage media like hard drives, or removable media like tape drives, USB drives shall be formatted if the media is to be reused.
- Low level formatting shall be done for hard disk drives of all desktops and laptops before re-using or sending them for maintenance.
- Expired or corrupted storage media like floppy, CDs or tape/optical media shall be degaussed or erased prior to its disposal.
- Erase/Uninstall sensitive data and licensed software totally from equipment prior to disposal.
- Media shall be physically destroyed prior to its disposal.
- Permanent media such as CDROM and floppy disk shall be defaced by scratching, broken in half, or shredded before being discarded.
- Hard-copy materials shall be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed

9. INFORMATION SYSTEM ACQUISITION, DEVELOPMENT and MAINTENANCE POLICY

9.1. Purpose

The purpose of this policy is to establish minimal security requirements for information system acquisition, development and maintenance.

9.2. Scope

This Policy contained within is applicable to all the authorized partners of The Tripactions including Interested Parties, Vendors and Third Party Service providers.

9.3. Policy Definitions

- The software development lifecycle shall contain information security as a fundamental requirement within.
- Applications shall go through functional testing after any change. The testing must be done before deploying the application in the production environment.
- Formal training program on secure coding shall be established for developers.
- All new information systems and services that are acquired, developed or enhanced must undergo security risk analysis using a formalized process, to ensure that appropriate security controls are identified and incorporated in them.
- Periodic code check/reviews shall be performed. Any vulnerability if encountered shall be documented.
- The developer shall not have access to production environment. Development and testing environments should redact all sensitive data or use de-identified data.
- In case of a developer needs access to production environment for testing purposes, prior approval from production manager shall be required.
- Any software intended for business use, which is not acquired through the formal procurement process (e.g. open source, freeware, shareware, etc.) must only be used after their respective

software licenses have been reviewed and the software is approved. Such changes are approved by Software Architect or System Architect and are scanned by GitHub dependency checker, which may also blacklist them for security reasons.

- Rules for the development of software and systems must be established and applied to developments within secure development is required to build up a secure service, architecture, software and system.

10. REMOTE ACCESS POLICY

10.1. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to the Organization's internal resources.

10.2. Scope

This policy applies to the users and devices that need access the organization's internal resources from remote locations.

10.3. Policy Definitions

- Remote access to the office's network shall be by approved secure methods, such as SSO and MFA.

11. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

11.1. Purpose

Development of knowledge, skills and attitudes enhances the performance of staff in their current tasks and prepares them for the emerging roles to which they will need to adapt. The purpose of this procedure is to create standard procedure for managing training in Tripactions.

11.2. Scope

This policy applies to the all Tripactions employees and services providers/contractors.

11.3. Policy Definitions

- All employees of the organization and contractors shall receive appropriate awareness education and training and shall be regularly updated on organization policies and procedures, as relevant to their job functions and PCI scope components.
- An information security awareness program shall aim to make employees and contractor aware of their responsibilities for information security.
- The awareness program shall be established in line with the organization security policies and procedures.
- Information Security awareness trainings programs for all employees shall be imparted through Intranet, security posters or induction

- Records of the training programs conducted shall be maintained
- Training shall happen periodically to meet Tripactions needs

12. OUTSOURCING POLICY

12.1. Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes.

12.2. Scope

This policy applies to the organization; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

12.3. Policy Definitions

- Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications
- Whenever possible, a bidding process might be followed to select between several service providers
- In any case, the service provider shall be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties
- Audits will be conducted to evaluate the performance of the service provider’s provisioning of the outsourced service, function or process. If the Organization has not enough knowledge and resources, a specialized company shall be hired to do the auditing
- A service contract and defined service levels must be agreed between the Organization and the service provider
- The service provider must get authorization from the Organization if it intends to hire a third party to support the outsourced service, function or process

13. ANNEX

1.1. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data shall only be accessed by authorized people.

External Service Provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs the organization’s approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.