Unleash the Talent Inside

Hitch
Information Handling
Policy

Contents

PURPOSE

Hitch is committed to maintaining the accuracy, confidentiality, and security of all Customer Data, Confidential Information and all information owned or processed by Hitch. Hitch is fully committed to compliance with applicable laws and regulations and industry best practices in handling Confidential Information.

Access to Confidential Information should be in accordance with the principle of “least privilege” and limited to only those who need to access such information in order to fulfill their professional responsibilities. All custodians of Confidential Information who have been granted such access should exercise care and judgment in accordance with this policy to ensure adequate protection of the information.

SCOPE

This policy applies to all Confidential Information owned by Hitch and/or processed by Hitch and to all Hitch employees, vendors, agents and affiliates who handle such information.

DEFINITIONS

"**Confidential Information**" means any information created by or disclosed to Hitch in writing including information which is not marked as "confidential" but which should, under the circumstances, be understood to be confidential by a person exercising reasonable business judgment. Confidential Information includes without limitation (a) matters of a technical nature such as trade secret processes or devices, know-how, data, formulas, inventions (whether or not patentable or copyrighted), specifications and characteristics of the products or services planned or being developed, and research subjects, methods and results; (b) matters of a business nature such as information about costs, profits, pricing, policies, markets, sales, suppliers, customers, product plans, and marketing concepts, plans or strategies; (c) matters of a human resources nature such as employment policies and practices, personnel,

compensation and employee benefits; (d) other information of a similar nature not generally disclosed by Hitch to the public; and (e) Customer Data.

"**Customer Data**" means electronic data and information submitted by or for customers (Organizations) of the Services including enhancement and output thereof derived from the use of the Services.

"Business Customer Data" means business contact details of Customer's personnel (e.g., employees, titles, employee identification numbers, agents and subcontractors).

POLICY

DISCLOSURE

Individuals should not disclose any Hitch Confidential Information that they obtain as a result of their authorization to access the information. Custodial obligations related to the appropriate handling of information are outlined in this policy.

COMPUTING REQUIREMENTS

Hitch Confidential Information should be protected whether it is being stored (on various media), transmitted (via network or email) or archived. Confidential and Restricted Information must be encrypted while at rest on any physical media and should always be encrypted in transit in accordance with Hitch Encryption Policy. Any system that Confidential or Restricted Information resides on must be password protected and follow Hitch's System Security Policy.

INFORMATION OWNERSHIP RESPONSIBILITIES

All Hitch Confidential Information should always be identified as Confidential and have a distribution or authorization list clearly marked. Managers are responsible for implementing the following good managerial controls:

- Granting and modifying access based on least privilege and only if job duties require access.
- Removing access when no longer needed.
- Creating and reviewing audit trails of access to restricted information.
- Regularly reviewing who has access to Confidential Information.
- Monitoring preventive controls for compliance.
- Educating end users regarding protection standards – set expectations.
- Ensuring that there is appropriate training of staff on proper handling of restricted information.
- Ensuring the information is properly secured during transmission, physical transport and storage.

All employees are responsible for maintaining the security and privacy of Confidential Information.

MANAGING ACCESS TO RESTRICTED INFORMATION

Strict control should be maintained regarding access to work locations, records, computer information, and other information. Individuals who are assigned keys, given special access or assigned job responsibilities in connection with the safety, security or confidentiality of such records, materials, or equipment should use sound judgment and discretion in carrying out their duties and will be held accountable for any wrongdoing or acts of indiscretion. Furthermore, information must not be divulged, copied, released, sold, loaned, reviewed, altered or destroyed except as properly authorized within the scope of this policy.

At the conclusion of their employment or affiliation with Hitch, individuals shall relinquish possession or control of all Hitch information. They shall also maintain the confidentiality of Hitch's information even after they have terminated their relationship with Hitch.

IDENTIFICATION, RETENTION, AND DISPOSAL OF CONFIDENTIAL INFORMATION

All Confidential Information must be retained and disposed of according to the terms described in this policy and in accordance with Hitch's Data Retention Policy.

INFORMATION CLASSIFICATION

Hitch has set guidelines for classifying, labeling and handling Confidential Information in the Information Classification Policy. For all Information the following color coding for the classification is allowed and encouraged for easy identification:

- **Public - Green**
- **Restricted – Blue**
- **Confidential - Red**

Please reference the "Information Classification Policy," the Information Classification Categories" and "Labeling and Handling" sections for more details.

INFORMATION HANDLING

The sensitivity guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Hitch's Confidential Information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Confidential Information in question. Digital information classified as Confidential or Restricted will be encrypted at rest and in transit at all times.

The handling requirements for each level of sensitivity includes the requirements of the lower levels of sensitivity.

PUBLIC INFORMATION

General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Hitch Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Hitch Proprietary" or similar labels at the discretion of your individual business unit or department.

If no marking is present, Hitch information is presumed to be "Hitch Confidential" unless expressly determined to be Hitch Public information by a Hitch employee with authority to do so.

Access: Hitch employees, contractors, people with a business need to know.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Hitch premises; electronic information should be expunged/cleared. Reliably erase or physically destroy media.

RESTRICTED INFORMATION

Trade secrets, other intellectual property, marketing information, operational, Business, financial, technical, and most personnel information.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Hitch Confidential" or "Hitch Proprietary", wish to label the information "Hitch Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Hitch employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution: No restrictions to approved recipients within Hitch, but should be encrypted or sent via a private link to approved recipients outside of Hitch premises. For information that must be sent on physical media outside the company the transfer must first be approved by the InfoSec team and encrypted in accordance with Hitch's encryption requirements. Physical deliveries must be carried by an employee or a reputable courier that can track the media all the way to delivery.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on Hitch premises; electronic information should be expunged/cleared. Reliably expunge or physically destroy media.

CONFIDENTIAL INFORMATION

Personally identifiable information(PII), Protected Health Information ("PHI"), Business Customer Information, Cusstomer information, customer tag configuration, information & technical information integral to the success of Hitch.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Hitch Confidential Information is very sensitive, you should label the information "Hitch Internal: Registered and Restricted", "Hitch Eyes Only", "Hitch Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Hitch Confidential Information need not be marked, but employees should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Hitch employees) designated with approved access on a need to know basis will be provided access.

Distribution: No restrictions to approved recipients within Hitch, but it is required that all Confidential Information be encrypted. For information that must be sent on physical media outside the company the transfer must first be approved by Hitch management and be encrypted in accordance with Hitch's Encryption Policy. Physical deliveries must be carried by an employee or a reputable courier that can track the media all the way to delivery.

Storage: Individual access controls are required to access electronic information. Physical security is also required and information should be stored in accordance with Hitch's System Security Policy.

Disposal/Destruction: In specially marked disposal bins on Hitch premises; electronic information should be expunged/cleared. Reliably expunge or physically destroy media.

INFORMATION ACCESS AUTHORIZATION AND DENIAL

Employees shall only handle information to which they have been granted access. The following are guidelines on granting, denying and revoking access.

GRANTING ACCESS

Access authorization ensures that persons authorized to use an information processing system have access only to the information they are authorized to access, and that Confidential Information will not be read, copied, altered or removed without authorization during processing or use. All system access must be tied to unique individual accounts. The use of shared accounts is strictly prohibited. Any exceptions must be approved by InfoSec in accordance with the Hitch's Exception Procedure. All access rights must be based on the person's role and job function within Hitch. The principle of least privilege must be strictly enforced for all Hitch systems, especially those that contain Confidential Information.

The information access control requirements are aimed at allowing only authorized persons to access the information which they are authorized to access, and to prevent the information from being manipulated or read by unauthorized persons.

Information access authorization is approved by management after a review of the application for access and a review of the security risks associated with access.

REVOKING PRIVILEGES AND/OR DENYING ACCESS

Information access authorization may be revoked or denied by management after a review of the application for access and a review of the security risks associated with access. Revocation of access will be implemented in accordance with the criteria below:

- Managers are primarily responsible for revoking employee's access to Hitch information system in the event of an employee's extended leave, transfer, or termination.
- In the event that a disabled user account needs to be re-enabled, the administrator will first confirm the identity of the requestor and the validity of the request through the employee's supervisor before enabling access.
- It is the responsibility of the employee's manager and the Human Resources department to notify relevant teams about an employee's extended leave, transfer, or termination and begin the process to disable access to Hitch's systems and information.
- Upon receiving such notification to revoke access either via email or other means, access management teams will initiate the process of revoking employee's access to information systems.
- Access to systems will be disabled promptly after the employee is terminated. This includes an employee's access to Customer Data, customer accounts, all of the data processing environments, email, intranet and other data processing systems.
- If the employee had access to configurations or stores that held private keys to systems, those systems keys will be rotated to newly created keys.
- System or security administrators shall regularly review system access for appropriateness.

EMPLOYEE SEPARATION

At the time of separation, the human resource (HR) department shall review the confidentiality commitments made by the employee in the *Hitch Confidential Information Agreement*. HR staff shall review signed confidentiality commitments to ensure that exiting employees understand the confidentiality obligations which remain in effect after separation.

REMEDIATION PLAN

In the event there is a breach of Confidential Information Hitch's InfoSec department will do the following:

1. Inform the information owner that the sensitive information has been compromised.
2. Perform an investigation of the compromise.
3. Inform the information owner and management of the investigation findings.
4. Work with departmental leadership to form an information handling remediation based on Hitch's Incident Response Plan.

ENFORCEMENT

Hitch's Chief Technology Officer and Chief Information Security Officer will coordinate with appropriate organizational entities on the implementation and enforcement of this policy.

Violation or non-compliance with this policy will be addressed in accordance with established Hitch disciplinary policies, procedures and enforcement authorities. Failure to comply with this or other related standards may result in disciplinary action up to and including termination of employment.

EXCEPTIONS

All Hitch employees, vendors and contractors must comply with this policy to the extent not in conflict with any applicable laws and regulations. However, technical or business constraints may dictate the need for an exception to this policy. For further information on how to submit an exception, please refer to Hitch's *Hitch Security Exception Procedure*.

VERSION HISTORY

Date	Status	Revision	Description	Reviewer/ Approver	Title
10/8/2020	V1 Final	1.1	Legal review, modified customer and platform users, data handling, business customer information inclusion	Tabetha Hineman Aki Estrella	Legal Counsel
9/10/2020	Draft	1.0	Draft	Jason Popp	Security Consultant

POLICY REVIEW

Policy Review requirements:	
Review Period	Annual
Retention Period	Life of the company (archived when superseded)
Next Review Date	November 2021
Location of policy	InfoSec Policies
Policy Keyword Search	Identity, Access, Risk, Audit, data processing, vendor agreements, PII, personal data, Confidential Information, Privacy
Related Policies/Procedures	• Information Security Policy • Information Classification Policy • Privacy Policy