DATA SECURITY POLICY

Introduction

The purpose of this document is to define the Info Salons Data Security Policy.

Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today's environment because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems create a unique vulnerability for our organisation.

This policy defines the Info Salons overall security and risk control objectives that we endorse. The premise for the policy can be stated as:

"Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorised entities."

This embodies the principle of least privilege.

This document forms part of your conditions of employment for employees, a part of the contractual agreement for vendors, suppliers, and third party processor or agents, hereafter referred to as vendors. All parties must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Breach of Policy and Enforcement

A breach of this policy could have severe consequences to Info Salons, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of the senior management of Info Salons. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of an Info Salons vendor, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Scope of the Policy

This policy applies to all Info Salons and customer data assets that exist in any Info Salons processing environment, on any media during any part if its life cycle. The following entities or users are covered by this policy:

- Full or part-time employees of Info Salons who have access to Info Salons or customer data.
- Info Salons vendors or processors who have access to Info Salons or customer data.
- Other persons, entities, or organisations that have access to Info Salons or customer data.

Data Life Cycle

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Usage

All users that access Info Salons or customer data for use must do so only in conformance to this policy. Uniquely identified, authenticated and authorised users must only access data.

Each user must ensure that Info Salons data assets under their direction or control are properly labelled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights.

Data Transmission

All users that access Info Salons or customer data to enable its transmission must do so only in conformance to this policy.

Where necessary, data transmitted must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the Info Salons policy on the use of cryptography.

The media used to distribute data should be classified so that it can be identified as confidential and if the media is sent using courier or other delivery method, it should be accurately tracked.

No data can be distributed in any media from a secured area without proper management approval.

Data Storage

All users that are responsible for the secure storage of Info Salons or customer data must do so only in conformance to this policy.

Where necessary, data stored must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the Info Salons policy on the use of cryptography.

Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights.

Data Disposal

Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights during the disposal process.

The Data Security organisation must develop and implement procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques.

Data Security Policy Statement

1. *Goals*

This policy has been written with the following goals in mind:

- To educate Info Salons users and vendors about their obligation for the protection of all data assets.
- To ensure the security, integrity, and availability of all Info Salons and customer data.
- To establish the Info Salons baseline data security stance and classification schema.

2. *Processing Environment*

The Info Salons processing environment that this policy applies to is comprised of:

- Applications – Application software is system or network-level routines and programs designed by (and for) system users and customers. It supports specific business-oriented processes, jobs, or functions. It can be general in nature or specifically tailored to a single or limited number of functions.
- Systems – A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data, which is used in a production or support environment to sustain

specific applications and business organisations in their performance of tasks and business processes.

- Networks – A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices) that are used to transport information between systems.

3. *Data Security Responsibilities*

The Data Security organisation is responsible for:

- Defining the security requirements, controls and mechanisms applicable to all data assets.
- Defining the methods and guidelines used to identify and classify all data assets.
- Defining the procedures for identifying data owners for all data assets.
- Defining the labelling requirements for all data assets.
- Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- Defining the procedures necessary to ensure compliance to this policy by all Info Salons users and vendors.
- Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognised in industry.

The Data Security, Network Operations and Systems Administration organisations must ensure the activation of all security mechanisms.

4. *Management Responsibilities*

Other organisations within Info Salons also have various responsibilities for ensuring compliance with this policy, such as:

- All individual organisations must ensure that staff complies with this policy.
- The Network Operations and Systems Administration organisations must ensure that adequate logs and audit trails are kept of all data access.

- The Data Security, Network Operations and Systems Administration organisations must ensure the activation of all security mechanisms.
- The Risk Management organisation is responsible for communicating business requirement and issues for business processes and the data those include, to ensure their correct data classification.
- The internal audit organisation is responsible for regularly evaluating the data classification schema for consistent application and use.

5. *Other Responsibilities*

Other organisations have responsibilities to comply with this policy, such as:

- All Info Salons agents, vendors, content providers, and third party providers that process customer data must have a documented security policy that clearly identifies those data and other resources and the controls that are being imposed upon them.
- All Info Salons agents, vendors, content providers, and third party providers that access the Info Salons processing environment and its data or provide content to it must have a security policy that complies with and does not contradict the Info Salons security policy.
- All agents, vendors, content providers, and third party providers must agree not to bypass any of our security requirements.

6. *Documentation*

This policy requires procedures be developed, managed and performed. As such, written documentation must be developed for all procedures necessary to fulfil this policy including:

- The management of all userids on all platforms.
- The management of all access control lists on all platforms.
- The execution and review of all audit trails.
- All incident response and reporting.

- All other tasks necessary to support this policy.

7. *Policy Review*

It is the responsibility of the Data Security organisation to facilitate the review of this policy on a regular basis. Because of the dynamic nature of the Internet, this policy should be reviewed annually. Senior management, Systems administration, and Legal should, at a minimum, be included in the annual review of this policy.

Data Content

The nature of specific data content that exists in the processing environment, and the controls that should apply to these, is dependent upon various factors. This policy does not mandate or endorse particular data content. Rather, the business decision process used to evaluate the inclusion or exclusion of particular data content should consider those items listed below. Regardless as to the specific data content that exists in the environment, all aspects of this policy must be enforced. Considerations for evaluating data content include:

- Legal and regulatory obligations in the locales in which we operate.
- Can privacy, confidentiality, security, and integrity of the data be ensured to the satisfaction of customers and legal authorities?
- Is it in line with our business goals and objectives?
- Do customers require or demand access to specific data content?
- What is common local practice?
- What rules govern the movement across international boundaries of different data content, and do we have in place controls to enforce these rules?

Data Classification

- Public Company Data – Public company data is defined as data that any entity either internal or external to Info Salons can access. The disclosure, use or destruction of Public company data will have limited or no adverse effects on Info Salons nor carry any significant liability. (Examples of Public company data include

readily available news, Company Name, Generic Terms in Interests and Industry Names & Codes.)

- Confidential Company Data – Confidential Company Data is information that is not to be publicly disclosed.
- Confidential Customer Data – Confidential customer demographic data is defined as data that only authorised internal Info Salons entities or specific authorised external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse effects on Info Salons and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by Info Salons (and others) over which they have custodial responsibility but do not have ownership.
- Public Customer Data – Public customer data is defined as data that any entity either internal or external to Info Salons can access. Public Customer Data is data classified that can be found on ASIC, ABN, Public Directories and Social Media

Non-disclosure Agreements

On occasion, data assets may need to be released to entities outside of Info Salons. When a legitimate business reason exists for releasing sensitive information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

Accountability

All network, system, and application events should be attributable to a specific and unique individual. It should be possible to attribute a responsible individual to every event through an identification service and to verify that the individual so assigned has been properly identified through an authentication service. It must also be possible to trace any event so as to reconstruct the time, place, and circumstances surrounding it through an audit service.

In this context identification refers to a security service that recognises a claim of identity by comparing a userid offered with stored security information.

Authentication refers to a security service that verifies the claimed identity of the user, for example a password. Auditability refers to a security service that records information of potential security significance.

Authorisation

All network, system, and application events must only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity, or from a job classification or administrative privilege based on that individual's identity. The principle of "least privilege" specifies that individuals only be granted permission for actions needed to perform their jobs.

Limiting actions to those properly authorised protects the confidentiality and integrity of data within the Info Salons processing environment.

In this context access control refers to a security service that allows or denies a user request based on privilege, group information, or context. Confidentiality refers to a security service that prevents disclosure of information to unauthorised parties while the information is in use or transit, or being storage or destroyed.

Availability

All permitted activity should operate with reliability. The data necessary to carry out such events must be readily retrieved and correct with high confidence. All results of an event must be completed, unless the event is aborted in its entirety. The results of an event should not depend in unexpected ways on other concurrent events. The security services themselves must be documented and easily administered.

In this context integrity refers to a security service that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery.

Core Security Principles

The information systems security architecture, policies, procedures, practices, and guidelines are developed in concert with the principles stated below. The following are the common core security principles recommended by industry best practices.

- Accountability Principle – The accountability and responsibility of information systems security should be explicit.
- Awareness Principle – Owners, providers, and users of information systems, and other parties should be informed about (or readily able to gain appropriate knowledge of) the existence and general extent of policies, responsibilities, practices, procedures, and organisation for security of information systems.
- Ethics Principle – Information systems and the security of information systems should be provided and used in accordance with the ethical standards applicable to your operating environment.
- Multidisciplinary Principle – Policies, responsibilities, practices, and procedures for the security of information systems should consider all relevant aspects of this effort, including technical (e.g. software and hardware engineering), administrative, organisational, operational, commercial, educational, and legal.
- Proportionality Principle – Security levels, costs, practices, and procedures should be appropriate and proportionate to the values of and degree of reliance on the information systems and to the severity, probability, and extent of potential for direct and indirect, tangible and intangible harm.
- Integration Principle – Policies, practices, and procedures for the security of information systems should be coordinated and integrated with each other and with other measures, practices, and procedures of the organisation to ensure a coherent system of security.
- Timeliness Principle – All personnel, assigned agents, and third party providers, should act in a timely, coordinated manner to prevent and to respond to breaches of the security of information systems.
- Reassessment Principle – The security of information systems should be reassessed periodically.

- Democracy Principle – The security of an information system should be weighed against the rights of customers, users, data owners, data custodians and other individuals affected by the system, and against your rights as the owners and operators of these systems.
- Certification and Accreditation Principle – Information systems and information security professionals should be certified to be technically competent and management should approve them for operation.
- Internal Control Principle – Information security forms the core of an organisation's information internal control system.
- Adversary Principle – Controls, security strategies, architectures, policies, standards, procedures, and guidelines should be developed and implemented in anticipation of attack from intelligent, rational, and irrational adversaries with harmful intent or harm from negligent or accidental actions.
- Least Privilege Principle – An individual should be granted only enough privilege to accomplish assigned tasks, but no more.

- Separation of Duty Principle – Responsibilities and privileges should be allocated in such a way that prevents an individual or a small group of collaborating individuals from inappropriately controlling multiple key aspects of a process and causing unacceptable harm or loss.
- Continuity Principle – Information security professionals should identify their organisation's needs for disaster recovery and continuity of operations and should prepare the organisation and its information systems accordingly.
- Simplicity Principle – Information professionals should favour small and simple safeguards over large and complex safeguards.
- Policy-Centred Security Principle – Policies, standards, and procedures should be established as a basis for managing the planning, control, and evaluation of information security activities.

Update 27 June 2022