
# Nectar Information Security Program

**Version 7.0**

**January 2020**

**Disclaimer**

All information in this document is subject to change without notice. Although the information is believed to be accurate, it is provided without guarantee of complete accuracy and without warranty of any kind. It is the user's responsibility to verify and test all information in this document and the user accepts full responsibility for all resulting outcomes.

**Trademarks**

SRSTP, UCMP-RIG, UCMP-DA, UCMP-CA, Converged Management Platform, UCMP, Vendor Knowledge Module, VKM, Vendor Quality Module, and VQM are trademarks of Nectar Services Corp.

Microsoft, Internet Explorer, Windows, Windows Server, Windows Vista, Win32, and the Microsoft logo, Windows logo, Windows logo (2002), Internet Explorer logo, Lync Logo and Windows start button, are registered trademarks. Lync 2010, Lync 2013, Skype for Business, Windows 2008, Windows 2010, Windows 2012 and Windows XP, are trademarks of Microsoft.

Oracle, Oracle logo, Java, Solaris, all trademarks and logos that contain Oracle, Solaris, or Java, and certain other trademarks and logos, are trademarks or registered trademarks of Oracle Corporation or its subsidiaries in the United States and other countries.

Cisco, Cisco Unified Communications Manager, Cisco Call Manager Express, Cisco Unity, Cisco Unity Express, Cisco Unified Border Element, are registered trademarks. Cisco UCM, Cisco CME, Unity, Unity Express, and CUBE, are trademarks of Cisco.

Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

# Document History and Version Control

| Version | Date | Author | Revision Notes | Section |
|---|---|---|---|---|
| 1.0 | December 2013 | Michael Ciano | Initial Policy Draft | All |
| 1.1 | January 2014 | Michael Ciano | Final Policy | All |
| 2.0 | January 2015 | Michael Ciano | Annual Review updated and release | All |
| 3.0 | January 2016 | Michael Ciano | Annual Review updated and release | All |
| 4.0 | January 2017 | J. Goldberg | Annual Review updated and release | All |
| 5.0 | January 2018 | J.E. Gerb;<br>D. Martinez | Annual Review updated and release | All |
| 6.0 | January 2019 | J.E. Gerb<br>M. Rosenthal | Annual Review updated and release | All |
| 7.0 | January 2020 | J.E. Gerb<br>M. Rosenthal | Annual Review updated and release | All |

# Table of Contents

# 1. Executive Summary

The Nectar Services Corp. (hereinafter, "Nectar Services") Information Security Program (ISP) is designed to protect information and critical resources from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information Technology (IT) security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of Nectar are met.

This plan governs the privacy, security, and confidentiality of Nectar data, especially highly sensitive data, and the responsibilities of departments and individuals for such data. IT security measures are intended to protect information assets and preserve the privacy of Nectar employees, partners, customers and other associated entities. Inappropriate use exposes Nectar to risks including cyber-attacks, compromise of network systems and services, and legal issues.

All users of the Nectar network are required to follow 'Acceptable Use of Assets Policy' and related, and are bound by this plan as well as other Nectar policies as terms of their employment. All employees share responsibility for the security of the information and resources in their respective departments.

# 2. Scope

The Nectar Information Security Program establishes and states the policies governing Nectar's IT standard and practices. These polices define Nectar's objectives for managing operations and controlling internal activities and those in the delivery of the Nectar Unified Communications Management Platform(UCMP) solution suite. These top-level policies represent the plans or protocols for achieving and maintaining internal control over information systems, application development, security vulnerability and assessment risks as well as compliance.

# 3. Policy

This Nectar Information Security Program ensures the confidentiality, integrity, and availability of data; defines the Security Development Lifecycle (SDL) and documents the information policies and procedures that support Nectar goals and objectives; and to allow Nectar to satisfy its legal and ethical responsibilities with regard to its IT resources.

Information security policies and procedures represent the foundation for Nectar's ISP. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout Nectar. Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business. When consistently applied throughout Nectar, these policies and procedures assure that the information assets are protected from a range of threats in order to ensure business continuity and maximize the return on investments of business interests.

This plan reflects Nectar's commitment to stewardship of sensitive personal information and critical business information, in acknowledgment of the many threats to information security and the importance of protecting the privacy of Nectar constituents, safeguarding vital business information, and fulfilling legal obligations.

This plan will be reviewed and updated at least once a year or when a material change has been identified.

# 4. Program Governance

The Security Oversight Committee is responsible for the governance of the Nectar Information Security Program and consists of the leadership, organizational structures, and processes to ensure that Nectar's information technology sustains and extends Nectar's strategies and objectives.

Executive Management has established the overall approach to governance and control by forming the Security Oversight Committee to provide strategic direction, ensure objectives are achieved, ascertain risks are managed appropriately, and verify that Nectar resources are used responsibly.

The Chief Information Security Officer shows his/her commitment by developing and implementing good internal controls as well as ensuring the promotion and awareness of IT Security requirements and plans throughout Nectar.

# 5. Policy Statement

Each department will protect Nectar resources by adopting and implementing, at a minimum, the security standards and procedures developed and approved by the Security Oversight
Committee as a cornerstone to the Information Security Program. All departments must meet the minimum standards. Departments are expected to adopt standards that exceed the minimum requirements for the protection of Nectar resources that are controlled exclusively within the Department.

Individuals within the scope of this policy are responsible for complying with this policy and the Department's policy, if one exists, to ensure the security of Nectar resources and assets.

# 6. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Nectar Services Corp. reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Nectar Services Corp. does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment or service, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Nectar reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her Manager, any other Manager or the Human Resources Department as soon as possible.

# 7. Information Security Program

Through this document and associated policies, Nectar has established, documented, and implemented an Information Security Program. The system is designed to result in improving the effectiveness of IT Operations, Software Development, Security and Vulnerability Risk Assessment, Incident Management and Compliance. This program has been implemented to ensure the confidentiality and integrity of Nectar information while maintaining appropriate levels of accessibility. In order to ensure the security and confidentiality of sensitive information and to protect against any anticipated threats or hazards to the security or integrity of data, Nectar has put in place all reasonable technological means, (i.e., security software, hardware) to keep information and assets secure. Key aspects of the program include:

## 7.1 Policy and Procedures

### 7.1.1 Information Asset Security Policies

Policies are implemented and enforced to assure the security, reliability, integrity, and availability of Nectar information assets. The Information Security Program contains policies and procedures that define:

- The risk assessment process.
- The enterprise-wide security controls.
- Security testing.
- Service provider oversight.
- Appropriate requirements for periodic review and updating of the Information Security Program.
- Appropriate requirements for reporting to Nectar Executive Management.
- The safeguarding of customer information.

### 7.1.2 Information Asset Security Procedures

Procedures are implemented to enforce security policies and assure the security, reliability, integrity, and availability of Nectar information assets.

### 7.1.3 Accidental or unauthorized events

Policies are implemented and enforced to protect Nectar information assets against accidental or unauthorized modification, disclosure, or destruction.

## 7.2 Policy Sanctions

### 7.2.1 Policy Sanctions

Nectar will implement sanctions against any employee and/or where applicable any third party who violates the written policies.

### 7.2.2 Policy Sanction Disciplinary Process

Assuming the action is inadvertent or accidental, first violations of information security policies or procedures will result in a warning. Second violations involving the same matter will result in a letter being placed in the involved worker's personnel file. Third violations involving the same matter will result in a five-day suspension without pay. Fourth violations involving the same will result in dismissal. Willful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including immediate dismissal.

## 7.3 Exceptions

### 7.3.1 Exceptions to Policies

Exceptions to information security policies are permissible only in those instances where a risk assessment examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the Information Owner or management, and where this form has been approved by both the Chief Information Security Officer and the Internal Audit.

### 7.3.2 Documented Policy Exception Process

All Nectar employees responsible for information security must submit a written request for exceptions to conform to information security policies. The Chief Information Security Officer must approve such exceptions.

### 7.3.3 Periodic Review of Documented Policy Exceptions

All documented and approved exceptions to Nectar security policy will be reviewed at least every six months.

## 7.4 Policy Distribution

### 7.4.1 Written Security Policy Documents

Nectar Management publishes written information security policies and makes them available to all employees and relevant external parties.

### 7.4.2 Annual Review of Applicable Security Policies

All Nectar employees and contractors must review and acknowledge acceptance of the Information Security policies, which apply to them at least on an annual basis.

### 7.4.3 Policy Document Classification

All Nectar security policy documents are labeled as CONFIDENTIAL and revealed only to Nectar workers and selected outsiders (such as auditors) who have a legitimate business need for this information.

## 7.5 Policy Review

### 7.5.1 Annual Review of Information Security Policy Documents

All Nectar written Information Security policy documents are be reviewed on an annual basis by the Security Oversight Committee.

### 7.5.2 Policy Review Input

The input to the Security Oversight Committee review of the Nectar Information Security policy will include information related to:

- Any feedback from interested parties.
- Results of independent reviews of the policy.
- To the status of preventive and corrective actions.
- To the results of previous management reviews.
- To process performance and information security policy compliance.
- Managing information security.
- Threat and vulnerability trends.
- Reported information security incidents.
- Recommendations provided by relevant authorities.

### 7.5.3 Policy Review Output - Process Management

The output from the Security Oversight Committee review of the Nectar Information Security policy will include:

- Any decisions and actions related to the improvement of the organization's approach to managing information security and its processes.
- Any decisions and actions related to the improvement of control objectives and controls.
- Any decisions and actions related to the improvement in the allocation of resources and/ or responsibilities.

## 7.6 Responsibility Assignment

### 7.6.1 Security Oversight Committee

The Security Oversight Committee composed of Senior leadership will meet quarterly to review the current status of information security at Nectar, approve and later review information security projects, approve new or modified information security policies, and perform other necessary high-level information security management activities. The Security Oversight Committee is responsible for maintaining organization-wide information security policies, standards, guidelines, and procedures.

### 7.6.2 Management Responsibility

Information security is a management responsibility, and decision-making for information security must not be delegated. While specialists and advisors play an important role in helping to make sure that controls are designed properly, functioning properly, and adhered to consistently, it is the Manager in charge of the business area involved who is primarily responsible for Information Security.

### 7.6.3 Clear Assignment of Control Accountability

Nectar Management does clearly assign and document accountability for every internal control at Nectar. This accountability must include sufficient transparency so that Executive Management will be kept informed about the effectiveness and efficiency of these same internal controls.

### 7.6.4 Information Ownership Assignment

The Chief Information Officer (CIO) will clearly specify in writing the assignment of Information Ownership responsibilities for those product systems, databases, master files, and other shared collections of information used to support production business activities.

## 7.7 Worker Information Security Roles

### 7.7.1 Three Categories of Responsibilities

To coordinate a team effort, Nectar has established three categories, at least one of which applies to each worker. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

### 7.7.2 Owner Responsibilities

Information Owners are the Department Managers, members of the Senior Management team, or their delegates within Nectar who bear responsibility for the acquisition, development, and maintenance of production applications that process Nectar information.
Production applications are computer programs that regularly provide reports in support of decision making and other business activities. All production application system information must have a designated Owner. For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

### 7.7.3 Custodian Responsibilities

Custodians are in physical or logical possession of either Nectar information or information that has been entrusted to Nectar. While Information Technology department staff members clearly are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

### 7.7.4 User Responsibilities

Users are responsible for familiarizing themselves with and complying with all Nectar policies, procedures, and standards dealing with Information Security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information.

Program Reporting

## 7.8 Program Reporting

### 7.8.1 Annual Security Program Report

Annual reports must be submitted to Nectar Management that includes information on:

- The status of the program.
- The updated risk assessment and analysis.
- Management decisions for the level of risk mitigation and residual risk accepted.
- Service provider oversight activities and status.
- The results of testing of key controls.
- Management's response to any identified deficiencies and recommendations for program changes.
- The independent validation of the information contained in the report.

## 7.9 Program Review and Maintenance

### 7.9.1 Annual Program Updates

The information security program must be updated and re-approved by Nectar Management annually or whenever there is a material change in the organization or infrastructure.

### 7.9.2 Risk Assessments

The Information Security program will be updated, as appropriate, based on the results of the organization's risk assessment and any risk assessment completed by a third party.

### 7.9.3 Information System Control Reviews — Independent

An independent and externally provided review of information systems security must be periodically obtained to determine both the adequacy of and compliance controls.

### 7.9.4 Change Considerations

The appropriate level of expertise will be applied to evaluate whether changes in the organization or infrastructure should trigger a change to the Information Security program. Changes that must be considered that could require an update to the information security program are the effect of changes in:

- Technology.
- The sensitivity of information.
- The nature and extent of threats.
- Nectar business arrangements, e.g., mergers, alliances, joint ventures.
- Customer information systems, e.g., new configurations, new connectivity, new software.

## 7.10 Security Program Compliance

### 7.10.1 Laws, Regulations and Contractual Requirements

For every Nectar production information system, all relevant statutory, regulatory, and contractual requirements must be thoroughly researched, explicitly defined, and included in current system documentation.

# 8. Definitions

**Confidential Information (Sensitive Information)** - Any Nectar Services Corp. information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product road-maps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Nectar from a third party under a non-disclosure agreement.

**Electronic Messaging System -** Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and text messaging.

**Information Asset** - Any Nectar Services Corp. data in any form, and the equipment used to manage, process, or store Nectar data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Objectionable Information or Material** - Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by national or international, federal, regional, provincial, state, or local laws.

**Partner** - Any non-employee of Nectar Services Corp. who is contractually bound to provide some form of service to Nectar.

**Password** - An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**User** - Any Nectar Services Corp. employee or partner who has been authorized to access any Nectar electronic information resource.

# 9. References

none

# 10. Related Documents

none