Third Party Security Management Policy

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 & 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 XP, Windows 2008, Windows 2010, Windows 2012, and Windows 2016 are trademarks of Microsoft.

CentOS Marks (CentOS 6 and CentOS 7) are trademarks of Red Hat, Inc.

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.

NICE Trading Recording is a trademark of NICE Systems.

Unigy is a registered trademark of IPC Systems, Inc.

FreeBSD and the FreeBSD logo are registered trademarks to The FreeBSD Foundation.

Sonus and Sonus logo are registered trademarks of Sonus Networks, Inc.

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

Approvals

Owner	Title	Date	Signature
James E. Gerb	Data Protection Officer	January 1, 2018	
James E. Gerb	Data Protection Officer	January 1, 2019	
James E. Gerb	Data Protection Officer	January 1, 2020	

Approved By	Title	Date	Signature
Marshall W. Rosenthal	General Counsel	January 1, 2018	
Marshall W. Rosenthal	General Counsel	January 1, 2019	
Marshall W. Rosenthal	General Counsel	January 1, 2020	

Document History and Version Control

Version	Date	Author	Revision Notes	Section
2.0	January 2015	P. Perry	Annual Review, updated and release	All
3.0	January 2016	M. Ciano	Annual Review, updated and release	All
4.0	January 2017	M. Ciano	Annual Review, updated and release	All
5.0	January 2018	J.E. Gerb M. Rosenthal D. Martinez	Annual Review, updated and release	All
6.0	January 2019	J.E. Gerb M. Rosenthal D. Martinez	Annual Review, updated and release	All
7.0	January 2020	J.E. Gerb M. Rosenthal D. Martinez	Annual Review, updated and release	All

Table of Contents

1. Purpose

This policy defines the requirements for the management of third-party services that handle sensitive information for Nectar Services Corp. (hereinafter, "Nectar") in any manner.

2. Scope

This policy applies to all Nectar computer systems and facilities, including those managed for Nectar customers. This policy applies to all employees, partners and third-parties with access to Nectar information assets.

3. Policy

3.1 Third-Party Security Requirements

3.2 Third-Party Risk Assessment

When using a third-party contractor to manage information processing facilities, all risks must be identified in advance, mitigating controls must be established, and all contractor expectations must be incorporated into the contract for these services.

3.2.1 Third Party Risk Assessment Team

Nectar must create a team of individuals responsible for performing third-party risk assessments. The team must consist of at least one member from the IT department and information security department.

3.2.2 Independent Security Control Reports

All agreements with third-party outsourcing organizations must stipulate that Nectar will annually receive a report expressing an independent opinion about the adequacy of the controls in use at the outsourcing organization.

3.2.3 Third-Party Access Terms And Conditions

Before any third-party is given access to Nectar systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager at the third-party organization and be approved by Nectar 's Information Security Manager and a senior Partner.

3.2.4 Third-Party Information Security Responsibilities

All Nectar business partners, suppliers, customers, and other business associates must be made aware of their information security responsibilities through specific language appearing in contracts that define their relationship with Nectar.

3.2.5 Security Requirements in Outsourced Network Services

All third-party agreements with network service providers must contain define security requirements so that external networks are at least as secure as Nectar internal networks.

3.2.6 Independent Security Scans of Outsourced Systems

For all Nectar product systems managed by third parties, Nectar must hire a qualified, independent third party to validate the security of these systems.

3.3 Third-Party Access Control

3.3.1 Third-Party Access To Internal Systems

Third-party access to any Nectar internal computer systems that are not clearly public must be approved in advance by a designated information security coordinator.

3.3.2 Third-Party User IDs

Before a user ID can be issued to a third party, documentary evidence of an information security system or process must be provided to, and approved by, Nectar 's Information Security Manager and the third party must agree in writing to maintain this system or process to prevent unauthorized and improper use of Nectar systems.

3.4 Information Exchange

3.4.1 Third-Party Sensitive Information Handling

All disclosures of secret, confidential, or private Nectar information to third parties must be accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used.

3.4.2 Third-Party Non-Disclosure Agreements

Prior to sending any secret, confidential, or private information to a third party for copying, printing, formatting, or other handling, the third party must sign a Nectar non-disclosure agreement.

3.4.3 Receiving Third-Party Information

If an agent, employee, consultant, or contractor is to receive secret or confidential information from a third party on behalf of Nectar, this disclosure must be preceded by the third-party signature of a release form approved by the Legal Department.

3.4.4 Third-Party Security Policy

Before any proprietary Nectar information is disclosed to a third party, this third party must sign a Nectar confidentiality agreement and submit a copy of its information security policy for approval by Nectar 's Information Security Manager

3.4.5 Information Handling At Contract Termination

If Nectar terminates its contract with any third-party organization that is handling Nectar sensitive information, this same third-party organization must immediately thereafter destroy or return all of the Nectar sensitive data in its possession.

3.4.6 Third Party Information Disposal

If the third-party destroys the information, Nectar must receive notice that the data was disposed according to the procedures established or approved by Nectar.

3.5 Third-Party Contracts

3.5.1 Control Measures in Outsourcing Contracts

All Information Technology outsourcing contracts must include specific words defining the control measures that will be provided and maintained. In addition, these contracts must specify a clear and expedient mechanism that Nectar management can employ to immediately update these controls without bureaucratic delays, protracted negotiations, or outsourcing firm management objections.

3.5.2 Outsourcing Contract Approvals

All information-systems-related outsourcing contracts must be reviewed and approved by the Information Security Manager who is responsible for ensuring that these contracts sufficiently define information security responsibilities, how to respond to a variety of potential security problems and the right to terminate the contract for cause if it can be shown that the outsourcing organization does not abide by the information-security-related contractual terms.

3.5.3 Reporting Third-Party Security Violations

All outsourcing contracts must stipulate that the third parties must notify Nectar immediately of any security incident likely to impact sensitive Nectar information under their control. Nectar will retain the right to aid in the investigation of these incidents.

3.5.4 Outsourcing Security Violations

All third-party outsourcing contracts must stipulate that the contract may be terminated due to information security violations by the outsourcing partner.

3.5.5 Outsourcing Firm Penalties

All outsourcing firm contracts must include fiscal penalties, approved by the Information Security Manager, for not maintaining information systems controls in a manner consistent with Nectar requirements.

3.6 Personnel Security

3.6.1 Right to Approve Personnel for Key Outsourced Positions

Nectar has the right to approve or reject any personnel hired by third-parties and which will perform duties on Nectar premises or handle Nectar sensitive data. This requirement must be included in any contracts with third parties performing IT or security-related duties for Nectar.

3.6.2 Non-Employee Background Checks

Temporaries, consultants, contractors, and other third-party organization staff must not be given access to sensitive information, or be allowed to access critical information systems, unless they have gone through a background check commensurate with the background checks given to regular employees.

3.6.3 Third-Party Notice Of Worker Terminations

If a terminated employee had authority to direct third-party contractors, or otherwise bind Nectar in a purchase or another transaction, then Nectar management must promptly notify all relevant third parties that the terminated worker is no longer employed by Nectar.

3.6.4 Personnel Cross Training with Key Outsourced Positions

All key technical positions staffed by outsourced personnel must provide cross-training for in-house personnel for at least six months before contract expiration.

3.7 Software Procurement

3.7.1 Software Integrity Statements

If procurement of third-party software is being considered, management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise the software's security, and will not require the modification or abandonment of controls found in the affected operating system.

3.7.2 Third-Party Software Development

All third parties who develop custom software on behalf of Nectar must be bound by a contract approved by the Information Security Manager. This contract, at a minimum, must include a clear and explicit definition of property rights, licensing arrangements, functional requirements, security measures, escrow arrangements, auditing rights, and testing processes.

3.8 Assessment, Monitoring and Audits

3.8.1 Critical Vendor Financial Review

The Chief Information Officer (CIO) or an individual designated by the CIO must review the financial condition of vendors providing or supporting critical Nectar production information systems annually.

3.8.2 Privacy Audit on Third-Party Systems Storing Sensitive Information

Nectar reserves the right to perform a privacy audit on any third-party production system that stores sensitive information on customers or employees.

3.8.3 Third-Party Auditing Agreements

All agreements dealing with the handling of Nectar information by third parties must include a clause granting permission to Nectar for the periodic auditing of the controls used for these information handling activities, and specifying the ways in which Nectar information will be protected.

3.8.4 Third-Party Notice Of Business And Technical Changes

Arrangements with information systems outsourcing firms must be structured such that Information Technology Department and Information Security Department management both receive notices of all material changes in the outsourcing firm business and technical environment. Such notices must be received well in advance of such changes actually taking effect.

3.9 Contingency Plans

3.9.1 Service Provider Contingency Plans

All contracts with web site hosting organizations, application service providers, managed systems security providers, and other information systems outsourcing organizations must include both a documented backup plan and a periodic third-party testing schedule.

3.9.2 Outsourced Production Systems Back-Out Plans

An effective and regularly-tested back-out plan, that permits Nectar to revert to internal processing and has been approved by the Information Security Manager, must be prepared and tested before any production information system processing may be transferred to an outsourcing organization.

3.9.3 Continuity Service Level Agreements with Third Parties

All agreements with third-parties, such as suppliers, service providers, and business partners, which could negatively impact the business processes of Nectar must define service level agreements and require minimum standards of contingency planning and preparation on the part of these third parties.

3.9.4 Priority Contingency Service in Agreements with Third Parties

All agreements with third-parties -- such as suppliers, service providers, and business partners -- upon which the business processes of Nectar will depend in an emergency or contingency and for whose attention Nectar will likely have to compete with other entities, should specify the priority of service that the Company will require from the third party.

3.9.5 Contract Failure Remedies

In addition, the contract language of these priority and Service Level Agreements (SLA) should specify remedies to Nectar in compensation for losses incurred by failure to put the Company's needs at the specified priority or service level.

3.10 Foreign Countries

3.10.1 Production Processing Outsourced To Foreign Companies

App

3.10.2 Sensitive Business Activities Performed In Foreign Countries

Research, development, manufacturing, assembly, and strategic planning related to those Nectar Services products which embody its most sensitive technology must not be performed in any foreign country. The definition of the products which fall into this category will be made by Nectar's Chief Legal Officer or General Counsel.

4. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Nectar 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 the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Nectar Services Corp. 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.

5. 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.

6. References

- MA 201 CMR 17.03 (1) - Security Program Requirements
- HIPAA: Security Management Process 164.308(a)(1)
- ISO 27002 - 6.1.1 Management commitment to information security

7. Related Documents