INFORMATION SECURITY PROGRAM POLICY

Policy #: IS-02
Version: 2.0
Effective Date: 5/8/2014
Last Update: March 2017
Contact: James Scheid (jscheid@revegy.com or 404.998.5713)

Revegy, Inc. 300 Galleria Parkway, Suite 1850, Atlanta, Georgia 30339
www.revegy.com

Table of Contents

1.0 Purpose & Scope

1.1 Purpose

This policy establishes the minimum requirements and responsibilities for the protection of Revegy information assets, preventing the misuse and loss of information assets, establishing the basis for audits and self-assessments, and preserving Revegy management options and legal remedies in the event of asset loss or misuse.

1.2 Scope

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

2.0 Policy

2.1 Programs

Information Security Program: Revegy must implement a comprehensive, written information security program that secures Revegy information assets in a manner commensurate with each asset's value as established by risk assessment and mitigation measures.

Information Privacy Program: Revegy must implement a comprehensive, written information privacy program that secures Revegy employee and customer personally identifiable information (PII) against unauthorized use or disclosure.

2.2 Policy & Procedures Requirements

Information Asset Security Policies: Policies must be implemented and enforced to assure the security, reliability, integrity, and availability of Revegy information assets. The information security program must contain 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 Revegy management
- The safeguarding of customer information

Information Asset Security Procedures: Procedures must be implemented and enforced to enforce security policies and assure the security, reliability, integrity, and availability of Revegy information assets.

Accidental or Unauthorized Events: Policies must be implemented and enforced to protect Revegy information assets against accidental or unauthorized modification, disclosure, or destruction.

2.3 Policy Sanctions

Policy Sanctions: Revegy must implement sanctions against employees and third parties who violate the written policies.

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

2.4 Exceptions

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 Information Security Manager and the Internal Audit Manager.

Documented Policy Exception Process: All Revegy employees responsible for information security must submit a written request for exceptions to conform to information security policies. Such exceptions must be approved by a member of the information security department.

Periodic Review of Documented Policy Exceptions: All documented and approved exceptions to Revegy security policy must be reviewed at least every six months.

2.5 Policy Distribution

Written Security Policy Documents: Revegy management must publish written information security policies and make them available to all employees and relevant external parties.

Annual Review of Applicable Security Policies: All Revegy employees and contractors must review and acknowledge acceptance of the information security policies which apply to them at least on an annual basis.

Policy Document Classification: All Revegy security policy documents must be labeled as CONFIDENTIAL – Internal Use Only and revealed only to Revegy workers and selected outsiders (such as auditors) who have a legitimate business need for this information.

2.6 Policy Review

Annual Review of Information Security Policy Documents: All Revegy-written information security policy documents must be reviewed on an annual basis by a team consisting (at a minimum) of members from the information security, legal, and human resources departments.

Policy Review Input: The input to the management review of the Revegy information security policy must 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

Policy Review Output–Process Management: The output from the management review of the Revegy information security policy must 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

2.7 Responsibility Assignment

Information Security Department Responsibilities: The Information Security Department is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.

Information Security Management Committee: An information security management committee composed of senior managers or their delegates must meet quarterly to review the status of information security at Revegy, approve and later review information security projects, approve new or modified information security policies, and perform other necessary high-level information security management activities.

Information Security Resources: Management must allocate sufficient resources and staff attention to adequately address information systems security.

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.

Clear Assignment of Control Accountability: Revegy management must clearly assign and document accountability for every internal control at Revegy. This accountability must include sufficient transparency so that top management is kept informed about the effectiveness and efficiency of these same internal controls.

Information Ownership Assignment: The Chief Information Officer (CIO) must 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.

2.8 Worker Information Security Roles

Three Categories of Responsibilities: To coordinate a team effort, Revegy 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.

Owner Responsibilities: Information Owners are the department managers, members of the top management team, or their delegates within Revegy who bear responsibility for the acquisition, development, and maintenance of production applications that process Revegy 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 are granted access, and approve requests for various ways in which the information is utilized.

Custodian Responsibilities: Custodians are in physical or logical possession of either Revegy information or information that has been entrusted to Revegy. 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 is not lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

User Responsibilities: Users are responsible for familiarizing themselves with and complying with all Revegy 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.

2.9 Program Reporting

Annual Security Program Report: Annual reports must be submitted to Revegy 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

2.10 Program Review & Maintenance

Annual Program Updates: The information security program must be updated and reapproved by Revegy management annually or whenever there is a material change in the organization or infrastructure.

Risk Assessments: The information security program must be updated, as appropriate, based on the results of the organization's risk assessment and any risk assessment completed by a third party.

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 with controls.

Change Considerations: The appropriate level of expertise must 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
- Revegy's business arrangements, e.g., mergers, alliances, joint ventures
- Customer information systems, e.g., new configurations, new connectivity, new software

2.11 Security Program Compliance

Laws, Regulations and Contractual Requirements: For every Revegy production information system, all relevant statutory, regulatory, and contractual requirements must be thoroughly researched, explicitly defined, and included in current system documentation.

3.0 Violations

Any violation of this policy may result in disciplinary action up to and including termination of employment. Revegy reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Revegy 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, Revegy 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.

4.0 Definitions & References

4.1 Definitions

Confidential Information (Sensitive Information): Any Revegy 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 roadmaps, 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 Revegy from a third party under a non-disclosure agreement.

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

Information Asset: Any Revegy data in any form, and the equipment used to manage, process, or store Revegy data, that is used during 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 Revegy who is contractually bound to provide some form of service to Revegy.

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

User: Any Revegy employee or partner who has been authorized to access any Revegy electronic information resource.

4.2 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

5.0 Approval, Ownership, & Revisions

5.1 Approval & Ownership

Owner	Title	Date	Signature
James Scheid	VP of Technology	05/08/2014	
Approved By	**Title**	**Date**	**Signature**
Mark Kopcha	CEO	05/08/2014	

5.2 Revisions

The following table shows the history of revisions that have been made to this document. This document will be reviewed on an annual basis.

Date	Description of Change	Version	Person Responsible
05/08/2014	Original document written and approved	1.0	James Scheid & Mark Kopcha
04/13/2015	Conversion to new format, annual review, and version update	2.0	James Scheid & Allison Smith
01/02/2017	Policy review, no content changes	2.0	James Scheid