Example
Tech Documentation

Information Security Program Charter

Updated: 2011.01.10 | Security classification: **Unclassified**

Contents

Introduction

Information is an essential Example asset and is vitally important to our business operations and delivery of services. Example must ensure that its informationassets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Example's Information Security Program will adopt a risk management approach to Information Security. The risk management approach requires the identification, assessment, and appropriate mitigation of vulnerabilities and threats that can adversely impact Example's information assets.

This Information Security Program Charter serves as the "capstone" document for Example's Information Security Program.

I. Scope

This Information Security Program Charter and associated policies, standards, guidelines, and procedures apply to all employees, contractors, part-time and temporary workers, and those employed by others to perform work on Example premises or who have been granted access to Example information or systems.

II. Information Security Program Mission Statement

Example Information Security Program will use a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures that address security objectives in tandem with business and operational considerations.

The Information Security Program will develop policies to define protection and management objectives for information assets. The Information Security Program will also define acceptable use of Example information assets.

The Information Security Program will attempt to reduce vulnerabilities by developing policies to monitor, identify, assess, prioritize, and manage vulnerabilities and threats. The management activities will support organizational objectives for mitigating, responding to and recovering from identified vulnerabilities and threats.

The Information Security Program will ensure that the Information Security Program Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to educate and train the individuals, groups, and partners covered by the scope of this Charter.

Example operates in the highly regulated fields of gaming (gambling) and payment card processing. Thus, a key activity of the Information Security Program will be to assure compliance with a range of international regulatory schemes.

III. Ownership and Responsibilities

The Chief Executive Officer (CEO) approves Example's Information Security Program Charter. The Information Security Program Charter assigns executive ownership of and accountability for Example Information Security Program to the Chief Technology Officer (CTO). The CTO must approve Information Security policies.

The CTO will appoint a Chief Security Officer (CSO) to implement and manage the Information Security Program across Example. The CSO is responsible for the development of Example Information Security policies, standards and guidelines, including PCI compliance. The CSO must approve Information Security standards and guidelines, and ensure their consistency with approved Information Security policies. The CSO also will establish an Information Security Awareness Program to ensure that the Information Security Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood across Example.

The Chief Security Officer (CSO) will establish a list of "Dependent Site Coordinators". The senior business or technical employee of each remote site or partner will be designated the Dependent Site Security Coordinator unless that person designates someone else. The role of the Dependent Site Security Coordinator includes submitting security requests, reviewing authorization reports, and being the main point of contact between the site/partner and Example's CSO.

Example's CSO is accountable for the execution of Example Information Security Program and ensuring that the Information Security Program Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood among Example sites, employees, and partners.

All individuals, groups, or organizations identified in the scope of this Charter are responsible for familiarizing themselves with Example Information Security Program Charter and complying with its associated policies.

IV. Enforcement and Exception Handling

Failure to comply with Example Information Security policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to Example Information Security policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the CSO. Exceptions shall be permitted only on receipt of written approval from the CSO or appropriate Example executive.

V. Review and Revision

Example Information Security policies, standards, and guidelines shall be reviewed under the supervision of the CSO, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness.

Approved: _____

Signature

Name

Title