Security and Privacy Overview

Overview

Evolution1 has formal Information Security and Privacy programs designed to meet the many requirements of state, federal and foreign laws and government and industry regulations. Relevant federal laws include but are not limited to the Gramm-Leach-Bliley Act, the Interagency Guidelines Establishing Information Security Standards, the Health Insurance Portability and Accountability Act (HIPAA), the Directive 95/46 EC of the European Parliament and of the Council of 24, the Australian Privacy Act of 1988, and the Personal Information Protection and Electronic Documents Act in Canada as well as the Payment Card Industry Data Security Standard (PCI DSS).

Each of these laws and regulations impose requirements for safeguarding personal information, such as Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Electronic PHI (ePHI), PII (Personally Identifiable Information), and Cardholder Data, through data security standards or guidelines.

Evolution1 takes the safeguarding of data very seriously. Each of our vendor, partner, and customer contracts contains language that binds both parties to comply with applicable privacy and security legislation and industry regulations. We use IIHI, PHI, ePHI, PII, and cardholder data only for authorized purposes, and use only minimum necessary data for the functions that we perform. In addition, our cardholder agreement (between our sponsor banks and the cardholder) restricts the bank's disclosure of data. Evolution1 has never sold any data and it is our intention to protect this data and never offer it for sale.

Evolution1 is PCI DSS Level 1 certified and SSAE16 SOC1 Type 2 certified.

Information Security Program

This IT Security Program is a compilation of a number of related policies that, when taken together, reflect a comprehensive approach to IT security that complies with PCI, HIPAA, Massachusetts Privacy Law and other requirements, as well as worldwide, generally accepted, best business practices.

Listed below are the policies that comprise the IT Security Program. Provision is also made for relevant procedures that support those policies. Both the policies and procedures are considered Controlled Documents and, as such, require the following:

- Unique number and title
- Management review
- Management approval
- Version control
- Retention of master documents in an Evolution1 limited access shared folder
- Distribution/availability to personnel

This document is confidential to Evolution1, Inc., and may not be used, copied or disclosed except with express prior written consent of Evolution1, Inc. It makes no warranties, expressed or implied in connection with its content. Copyright © 2013 Evolution1, Inc. All rights reserved. Business processes protected under US Patents 7,174,302, 7,197,468 and 7,680,679 with additional patents pending.

Topics covered by our Information Security Policies and Procedures are as follows:

Policy 01-01 PL: IT Security Program
Procedure 01-01.01 PR: Managing Controlled Documents
Policy 01-02 PL: Acceptable Use of Information Resources
Policy 01-03 PL: Risk Management
Form 01-03.01a FM: Using Personal Wireless Devices to Access the Network
Policy 02-01 PL: Account Access Management
Procedure 02-01.01: PR Account Access Management
Policy 02-02 PL: Remote Access
Policy 03-01 PL: Physical Security and Access
Procedure 03-01.01 PR: Physical Security and Access
Policy 04-01 PL: System Acquisition, Development and Change
Procedure 04-01.01 PR: System Life Cycle (SLC) Framework
Procedure 04-01.02 PR: Change Management
Procedure 04-01.03 PR: Security Code Review Guidelines
Policy 05-01 PL: Network Device Configuration
Procedure 05-01.01 PR: Network Device Hardening
Procedure 05-01.02 PR: Network Device Accepted Protocols
Procedure 05-01.03 PR: Network Device Naming Conventions
Policy 05-02 PL: Server and Computer Configuration
Procedure 05-02.01 PR: Server and Computer Hardening
Procedure 05-02.02 PR: Patch Management and Vulnerability Assessment
Procedure 05-02.03 PR: Trusted Access Standards for Devices
Procedure 05-02.04 PR: Server Naming Conventions
Policy 05-03 PL: Anti-Virus and Anti-Spyware Management
Policy 05-04 PL: Audit Logging and Monitoring
Procedure 05-04.01 PR: Audit Logging and Monitoring
Policy 05-05 PL: Backup and Recovery
Procedure 05-05.01 PR: Backup and Recovery
Policy 05-06 PL: Contingency Planning
Policy 05-07 PL: IP Blocking
Procedure 05-07.01 PR: IP Blocking
Policy 06-01 PL: Information Protection
Procedure 06-01.01 PR: Encryption
Procedure 06-01.02 PR: Key Management
Policy 06-02 PL: Retention
Procedure 06-02.01 PR: Retention
Policy 07-01 PL: Asset Management
Procedure 07-01.01 PR: Asset Management
Policy 08-01 PL: Problem and Security Incident Management
Procedure 08-01.01 PR: Problem-Security Incident Management
Policy 09-01 PL: Third Party Management
Policy 10-01 PL: Data Protection – DLP
Policy 11-01 PL: Provisioning of Security Certificates
Procedure 11-01.01 PR: Security Certificate Implementation
Policy 12-01 PL: Corporate Email Security

Due to the proprietary nature of these policies and procedures, it is our policy not to share them outside the company in their entirety.

Updates and Reviews

- IT policies and procedures are made available to all Evolution1 employees
- IT policies and procedures are maintained current to reflect changes to the business environment, IT environment or legal, regulatory and PCI requirements.
- All IT policies and procedures are reviewed annually. Any approved change to a policy or procedure in a given year can be considered its annual review for that year.

Training and Awareness

- Training on IT policies and procedures are conducted in accordance with Evolution1 employee job function and their access to information assets and privacy information.
- Periodic information security reminders are published to all Evolution1 employees regarding employee responsibilities for protecting information assets and privacy information.

Disciplinary Actions for Violation

- Violation of this policy may result in disciplinary action which may include termination for Team Members and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of Evolution1 Information Technology Resources access privileges, civil, and criminal prosecution.