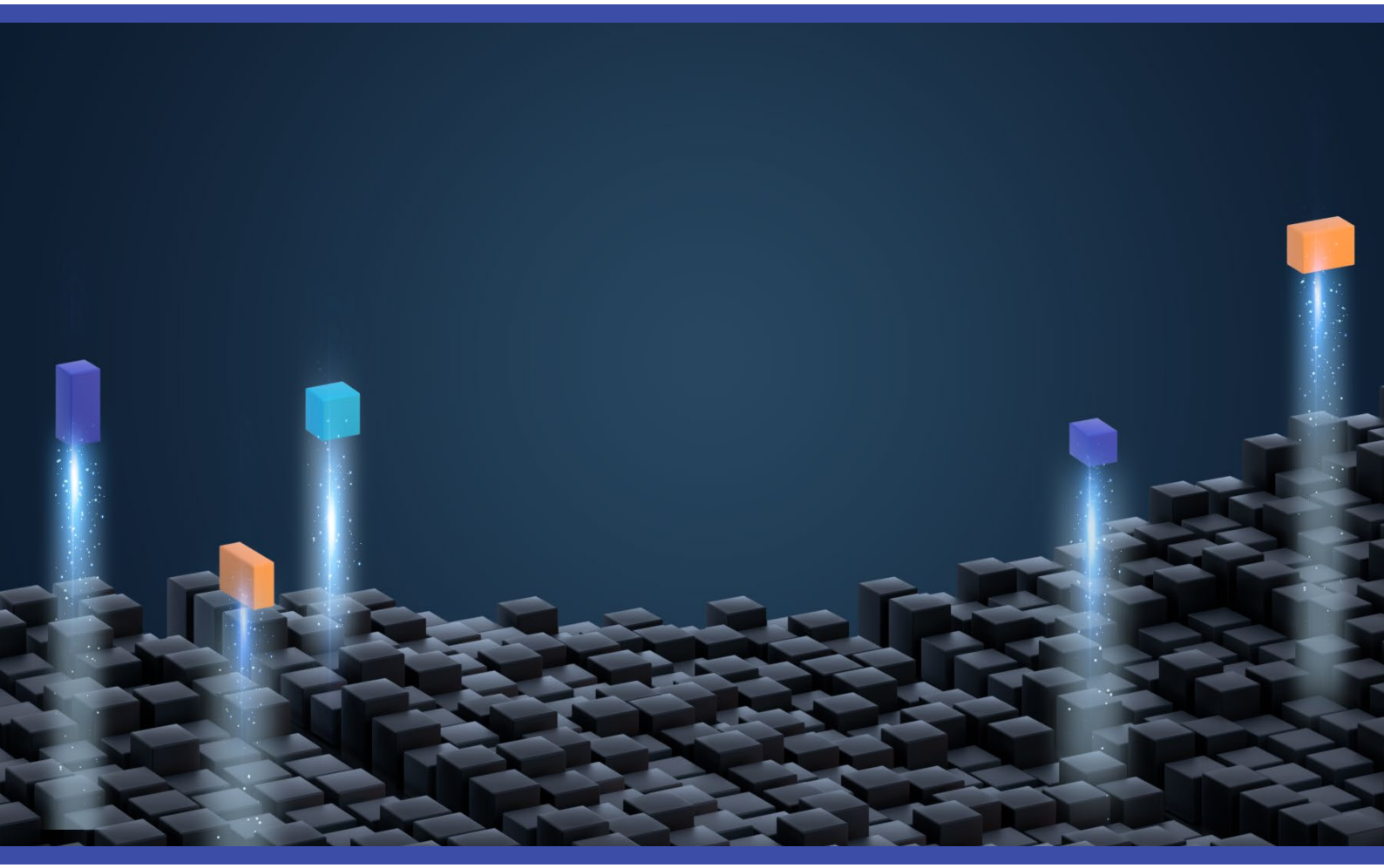
OpenLegacy
Digital to the Core

OpenLegacy Data Protection Policy

March 2021



Contents

1 Introduction....1
2 Scope....1
3 Information Security Controls – General....1
4 Personnel, Communications and Operations Management....2
5 Computer System Security Requirements....2

Disclaimer

The information contained in this document, and this document itself, is for internal OpenLegacy use and reference solely. The Policies and Procedures contained herein, and this document itself, in whole or in any part, cannot be quoted directly or indirectly, referenced, copied, or attached into any OpenLegacy Client or Partner Agreement.

If they are presented or provided to a client or partner in any electronic or printed format, it will be solely and expressly for informational and/or assessment purposes.

© 2021 OpenLegacy Inc. All Rights Reserved.

1 Introduction

OpenLegacy is committed to achieving and maintaining the trust of our clients and partners (hereafter 'Client'). Integral to this mission is providing robust security and data protection mechanisms that provide both OpenLegacy and the client with mechanisms to ensure the security of data across our Products and Services.

This Information Protection Policy ("Policy") provides clients with a standard set of security safeguards used in the performance of OpenLegacy Products and Support Services purchased under the Master Subscription Agreement ("Agreement").

2 Scope

a) Definition.
For purposes of this Policy, the term "Data" shall mean Confidential Information and any data or other information provided by client to which OpenLegacy has or has had access in connection with the Software ("Products") or professional consulting services and support and maintenance ("Support Services") purchased under the Agreement.

b) Security and Data Protection Obligations
This Policy applies to:

i. OpenLegacy and its personnel who may access Data in the course of providing the Products or Support Services;
ii. all Data collected, stored, processed or transmitted by client using the software;
iii. all information systems owned or operated by OpenLegacy that are used in connection with the provision of the Support Services. This Policy applies to any subcontractors and their personnel to the same extent as it applies to OpenLegacy.

3 Information Security Controls – General

a) Security Control Program
OpenLegacy represents and warrants that it developed, implemented, and maintains a comprehensive written information security control program ("Program") applicable to the Products, that contains administrative, technical, and physical safeguards that are appropriate to the need for security and confidentiality of the Data. The safeguards contained in such Program are and shall remain consistent with the safeguards set forth in any state or federal regulations applicable to the Products and practiced by top tier providers of services like those provided by OpenLegacy.

b) Information Security Controls
At Client's request, OpenLegacy shall provide Client with written evidence of its Program, covering all information systems, equipment and facilities used in connection with the provision of the Products.

© 2021 OpenLegacy Inc. All Rights Reserved.

4 Personnel, Communications and Operations Management

Without limiting the generality of the above, the OpenLegacy Program includes:

a) A designated team responsible for maintaining OpenLegacy information security controls.

b) Identifying, assessing and promptly correcting reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any Data, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
   - ongoing employee training (including temporary and contract employee) , including electronic correspondence behavior and personal online security
   - employee compliance with policies and procedures
   - means for detecting and preventing security system failures
   - Security policies for employees relating to the access of Data
   - Imposing and enforcing disciplinary measures for violations of the comprehensive information security controls
   - Preventing terminated employees from accessing any Data
   - Overseeing subcontractors by taking reasonable steps to select and retain third-party service providers that can maintain appropriate security measures to protect Data consistent with these Information Security and Data Protection obligations
   - Regular monitoring to ensure that the Program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Data and upgrading information safeguards as necessary to limit risks.
   - Reviews of the security measures, at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Data and/or specific warnings from Law Enforcement Agencies or other authorized bodies.
   - Notification to Client of any breach, or actual non-compliance by OpenLegacy of any applicable Data protection law or any provision of this Policy as soon as reasonably possible after becoming aware of such breach or actual non-compliance.
   - Documentation and recording of responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Data.

5 Computer System Security Requirements

The OpenLegacy Program includes commonly requested security protocols that include the following elements:

a) Secure user authentication protocols including:
   - Adherence to the principles of “Deny All”, “Need to Know” and “Least Privilege”;
   - Strong control of User IDs and other identifiers

© 2021 OpenLegacy Inc. All Rights Reserved.

- Secure method of assigning and selecting passwords, with appropriately strong parameters, as well as the use of unique identifier technologies
- Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of Data they protect
- Access is restricted to active users and active user accounts only
- Access is blocked to user after multiple unsuccessful attempts to gain access to a system

b) Secure access control measures that:

- Restrict access to records and files containing Data to only those who need such information to perform their job duties
- Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls

c) Encryption is used to:

- Protect transmitted records and files containing Data that will travel across public networks, and, if applicable, encryption of all Data to be transmitted wirelessly, with encryption in all cases at a strength that is commercially reasonable given the nature of the data transmitted and the transmission method(s).

d) Systems are monitored for unauthorized use of or access to Data.

e) Encryption is in place on all Data stored on laptops or other portable devices.

f) For files containing Data on a system that is connected to the Internet, there must be up-to-date firewall protection and operating system security patches designed to maintain the integrity of the Data.

g) Up-to-date versions of system security agent software, which must include malware protection and up-to-date patches, or a version of such software that can still be supported with up-to-date patches, and is set to receive the most current security updates on a regular basis.

h) Education and training of employees on the proper use of the computer security system and the importance of Data security.

© 2021 OpenLegacy Inc. All Rights Reserved.