Confidentiality Policy

Privo IT

April 2020

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	C1.1, C1.2

Table 2: Document history

Date	Comment
November 19, 2019	Initial document

1 Purpose and Scope

a. This policy outlines expected behavior of employees to keep confidential information about clients, partners, and our company secure.

b. This policy applies to all employees, board members, investors, and contractors, who may have access to confidential information. This policy must be made readily available to all whom it applies to.

2 Background

a. The company's confidential information must be protected for two reasons:
   i. It may be legally binding (i.e. sensitive customer data)
   ii. It may be fundamental to our business (i.e. business processes)

b. Common examples of confidential information in our company includes, but is not limited to:
   i. Unpublished financial information
   ii. Customer/partner/vendor/external party data
   iii. Patents, formulas, new technologies, and other intellectual property
   iv. Existing and prospective customer lists
   v. Undisclosed business strategies including pricing & marketing
   vi. Materials & processes explicitly marked as "confidential"

c. Employees will have varying levels of authorized access to confidential information.

3 Policy

a. *Employee procedure for handling confidential information*
   i. Lock and secure confidential information at all times
   ii. Safely dispose (i.e. shred) documents when no longer needed
   iii. View confidential information only on secure devices
   iv. Disclose information only when authorized and necessary
   v. Do not use confidential information for personal gain, benefit, or profit

vi. Do not disclose confidential information to anyone outside the company or to anyone within the company who does not have appropriate privileges

vii. Do not store confidential information or replicates of confidential information in unsecured manners (i.e. on unsecured devices)

viii. Do not remove confidential documents from company's premises unless absolutely necessary to move

b. *Offboarding measures*

i. The Hiring Manager should confirm the off-boarding procedure has been completed by final date of employment.

c. *Confidentiality measures*

i. The company will take the following measures to ensure protection of confidential information:

1. Store and lock paper documents
2. Encrypt electronic information and implement appropriate technical measures to safeguard databases
3. Require employees to sign non-disclosure/non-compete agreements
4. Consult with senior management before granting employees access to certain confidential information

d. *Exceptions*

i. Under certain legitimate conditions, confidential information may need to be disclosed. Examples include:

1. If a regulatory agency requests information as part of an audit or investigation
2. If the company requires disclosing information (within legal bounds) as part of a venture or partnership

ii. In such cases, employee must request and receive prior written authorization from their hiring manager before disclosing confidential information to any third parties.

e. *Disciplinary consequences*

i. Employees who violate the confidentiality policy will face disciplinary and possible legal action.

ii. A suspected breach of this policy will trigger an investigation. Intentional violations will be met with termination and repeated unintentional violations may also face termination.

iii. This policy is binding even after the termination of employment.

f. *Sensitive Information*

Sensitive Information is defined as information that should be protected against unwarranted disclosure. Sensitive information must have the same treatment as Confidential Information. Access to sensitive information should be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations. Sensitive Information includes all data, in its original and duplicate form, which contains:

```
i. Personal Information, as defined by the Massachusetts privacy law (see section "Massachus

i. rotected Health Information, as defined by the Health Insurance Portability and Accountab

i. Confidential and proprietary information of Privo and its customers including any informa

i. Customer passwords, credit card numbers, or account numbers
```