DATA MANAGEMENT POLICY

INTRODUCTION

Sensorpro operates in an increasingly complex, data-oriented, environment which requires the key data assets be managed correctly to underpin client confidentially, security and integrity. This document provides a corporate framework with defined roles and responsibilities for Data Management.

DATA STEWARDS, EXPERTS AND USERS.

Every data source and Dataset must have a designated Data Steward. A Data Steward is responsible for the data quality, security and availability of the data assigned. The data steward will be familiar with the policies and controls associated with a particular partner or client environment and understands the process that needs to be adhered to. Data Experts and Users must comply with directives from a Data steward. All Data Stewards, Experts and Users should clearly understand this policy, the Privacy policy and Acceptable Usage Policy.

POLICY

Our platform is hosted in a number of data centres and environments that are subject to this Data Management policy. Each of our partners have their own policy that will be co-ordinated by the appropriate Data Steward. The following partners have specific guidelines on working with Data from their environments: Epsilon Interactive, Epicor and ExactTarget.

Our own datacentre is owned by Telecity.ie and operated by Blacknight. Access to the center must be authorised by Blacknight and via the Data Steward only. No removable media may be brought into the center. No personal filming or social media activity is permitted in the center. The center has full CCTV and records all check-in and out activity. When in the center, you will be with an authorised rep from Blacknight. You must only work on our designated cage and not remove or bring in any unauthorised items of any kind. Any replaced server drives must be securely wiped.

CLIENT DATA

The integrity of client data is our number one concern. Data Stewards, Experts and Users must be vigilant at all times to ensure that data is available only to authorised users. We expect our staff to assist clients with understanding policy implementation and best practice. Please note the following points in your day to day work:

1 Client logins should be IP locked down where possible. This ensures that access to the client account is from a known physical location.

2 All login links should be deployed as https://

3 Passwords must be 8 characters long and are forced-change on a cycle set at system level. Never include passwords in an email with other login credentials. If possible email the login credentials but send the password by SMS. Note that after 3 invalid login attempts the account will be locked and the customer must contact the Helpdesk directly.

4 All export/import data must use SFTP and only in accordance with partner/client policy. From time to time, a client will ask to email data for import or export. It is Helpdesk policy to refuse this activity and you should ask clients to refrain from such activity.

5 For on-premise installations, the Data Steward must be satisfied that the Customer datacentre operates to minimum Tier 3 with appropriate ISO27001 Information Security and ISO22301 Business Continuity standards. The datacenter should provide evidence of the following standards: Uptime Institute Tier Standard:Topology, TIA-942 Telecommunications Infrastructure Standard for Data Centers, and BICSI 002-2011 Data Center Design and Implementation Best Practices.

6 For on-premise installations ensure appropriate certificate purchase and installation for https://

DATA-BREACH GUIDELINES

The Customer should be made aware of their responsibility for data and that they have their own Data policy in place. In the event of a breach, the customer must follow the guidelines set out by the Data Commissioner here: http://www.dataprotection.ie/docs/Breach-Notification-Guidance/901.htm

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) place specific obligations on providers of publicly available electronic communications networks or services to safeguard the security of their services. These obligations are:

At a general level, such undertakings are required to have in place appropriate technical and organisational measures to keep personal data safe and secure. More specifically, providers of publicly available electronic communications networks or services are required to:

have a security policy in place (and be in a position to demonstrate that the security policy has been implemented and kept relevant); ensure that personal data can only be used by authorised personnel for authorised purposes; and protect personal data against unlawful use or access. In case of any particular risk to the security of the network, providers of publicly available electronic communications networks or services must provide information to subscribers without delay about the risks and any possible remedies (including the likely costs involved) even where the proposed measures are outside the direct control of the undertaking.

In case of a personal data security breach affecting even one individual, providers of publicly available electronic communications networks or services must without undue delay: notify the Office of the Data Protection Commissioner of the breach (even in circumstances where it considers the data would be unintelligible to third parties) including a description of the measures to be taken to address the breach; and notify any individual that may be adversely affected by the breach. It is not necessary to notify individuals if the Office of the Data Protection Commissioner is satisfied that the data would be unintelligible to third parties. The Commissioner can require an undertaking to notify individuals if the undertaking does not consider it necessary.

Any notification to individuals affected by a personal data security breach must contain:

an outline of the breach; a contact point for obtaining more information; and recommended measures to mitigate any possible adverse effects from the breach. Additionally, providers of publicly available electronic communications networks or services must maintain an inventory of personal data breaches which can be checked by the Office of the Data Protection Commissioner.