SENSORPRO

Data Security Policy

CONTENTS

1.1 Access Control 1
1.2 Use Of Privileged Utility Programs 1
1.3 Access Authentication 2
1.4 Clear Desk / Screen 2
1.5 Data and Retention 3
1.6 Server Security 3
1.6.1 Access Control 3
1.6.2 Configuration 3
1.6.3 Review 4
1.7 Portable devices 4
1.8 Disposal of equipment 5
1.9 Physical Security 5
1.10 Password Management 5

1.1 ACCESS CONTROL

- Employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- Access to data is on a need to know basis, or as instructed by customer.
- Every employee needs to apply effort and intelligence in maintaining ethics value.
- Employees must disclose any conflict of interests regard their position within SensorPro.
- Employees will help SensorPro to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.
- Employees should consider the following questions to themselves when any behavior is questionable:
- Is the behavior legal?
- Does the behaviour reflect SensorPro values and culture?
- Could the behaviour adversely affect company stakeholders?
- Is the data secure?

1.2 Use Of Privileged Utility Programs

The use of utility programs that might be capable overriding system and application controls are tightly controlled.

Access to such programs should be granted on a case by case basis, and would generally facilitate a customer request or to troubleshoot a customer issue.

1.3 Access Authentication

Access to data should be protected in the following ways:

- Complex password being a minimum of 8 characters using a mix of letters and numbers and characters which are not a-z
- After 3 invalid attempts account is locked out and this account can only be unlocked by support.
- Access to web sites should be over secure channel SSL.
- Where possible login should be locked down by ip address.
- Each account login attempt failed or successful is recorded including ip address and browser.
- All computers should have password protect screen savers.
- Users are forced to change password every 3 months.
- Password should be encrypted at rest. The encryption key should vary depending on the user, thus avoiding a one key for all.
- Only functions required to do the job should be available to the logged in user.

1.4 Clear Desk / Screen

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Clear desk, leaving any documents which may contain sensitive information they should be kept in desk or cabinets.
- Clear screen, do not leave any sensitive information unattended on screen. Screen should be locked if leaving your desk.

1.5 Data and Retention

Databases

Databases are backed up for the purposes of disaster recovery.

- **Schedule:** Nightly, saved to a second disk array within the data centre.
- **Backup Type:** Full database
- **Retention:** Backups are retained for one day, after which they are automatically deleted.

Images

Images, which are used in newsletters are backed nightly for the purposed of disaster recovery.

- **Schedule:** Nightly, saved to a second disk array within the data centre.
- **Backup Type:** Changed images
- **Retention:** A single copy of the images are maintained at all times.

MTA Ironport

- Ironport configuration is backed up after each OS upgrade. The configuration is exported as an xml document which is stored on a bit locked drive.

Contract Termination

On notification of contract termination:

- Organization will be deleted this will remove the following:
  - All campaign/contact data from the database.
  - All images from the image store
  - Any uploaded documents

The data will be removed as soon as possible but no later than 30 days after notification.

1.6 Server Security

1.6.1 Access Control

Data centre access is requested via support with Blacknight. This must be request at least 24 hours in advance. Email help@blacknight.ie or phone 1850 929 929 to request access.

- Photo ID required on arrival.
- Rack C08.
- Addition or removal of hardware must be indicated in advance of visit.
- **Server access:** is via remote desktop which locked down by IP address only allowing access from the office at Lonsdale Road, and internally from the data centre.

1.6.2 Configuration

- **Anti Virus:** Servers run ESET NOD32.

- **Firewall:** Servers are protected by firewall - only the ports which are required for the operation of the server should be opened.

- **Web/Server monitoring:** Sites are monitored via Pingdom with SMS and email alerts.

- **Log Files & Audit Trails:**
  - Web Server Application log files are saved and archived, in case future analysis of the files is required.
  - Windows log files are saved and archives in case future analysis is required.

- **Patch Management:** "Important" server patches are applied ASAP, the following Friday after the security the patch becomes available. "Optional" patches are scheduled and applied at a convenient time.

- **Web Server Penetration Testing:** Penetration testing is carried out on a replica web site, on the same hardware to test for vulnerabilities, this testing will be carried out as follows:

  - Penetration testing is run on a replica site which is an exact copy of the live system. Running penetration test of live site can have a detrimental effect on the site performance.

  - Penetration testing should be carried out as follows:
    - After deployment software modifications
    - Once a quarter at a minimum

  - Remediation of issues:
    - Identify false positives
    - Fix & deploy
    - Or revert to previous software version

  - Tools currently used Acunetix / Zap.

1.6.3 Review

A weekly of all servers a manual review of the following items.

- Disk space, disk status
- Review log files windows and web server log files for unusual activity
- Review of any pending windows patches
- Database health review
- Antivirus status
- Pingdom response times review

1.7 Physical Security

See Blacknight Data Centre Attestation document.

1.8 Portable devices

Laptops, USB keys, smart phones and other forms of portable device are especially vulnerable to theft and accidental loss. Where it is considered essential to store data on a portable device, these devices should be encrypted. In the case of smart phones, a strong password should be required at start up and also after several minutes of inactivity. When such a device is lost steps should be taken immediately to ensure that the remote memory wipe facility is activated. Staff allocated such devices should be familiar with the relevant procedures.

1.9 Disposal of equipment

When equipment has reached end of life or is going to be recycled for another purpose within the organization.

- IT will securely erase all storage mediums by low level format. If the item is being decommissioned, the hard drives are destroyed.
- In order for equipment to be disposed of via skips, dumps, landfill, electronic recycling etc. the hard drives must be removed.
- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- IT will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

1.10 Password Management

Passwords are the primary mechanism to protect data and as such the following rules should be adhered to:

- Passwords should always be strong minimum of 8 characters long with mix of characters and numbers and at least one punctuation character.
- Passwords should never be written down, and should be managed through password manager if they cannot be remembered.
  - The password management system should enforce complex password and give warning if weak passwords are used.
- Server passwords should be maintained within a password management program.

- Where passwords have been reset, and need to be sent to a customer, the password if possible should be sent via SMS message, if this is not possible it should be sent in a lone email with no other information relating to the login process.
- Password reset requests should be received via email to allow matching of company and user to account.