Information Security Policy

1.0 Overall Objectives

Information Security is of prime importance for both Digital Spotlight Limited and our clients. This document defines what we consider sensitive information covered by this Information Security Policy, the risks to that information and the policies we have implemented to minimise those risks.

2.0 Sensitive Information

Sensitive information consists of:

- Commercially Sensitive Information owned by Digital Spotlight Limited.
- Commercially Sensitive Information owned by a client.
- Information covered by a clients Non-Disclosure Agreement (NDA)
- Financial Information owned by Digital Spotlight Limited.
- Digital Spotlight Limited Personnel Information.
- Client test and live data.
- Software code and other digital assets both published and under development.
- Security information including usernames and passwords.
- Software Applications.

This information may be in either digital format or paper documents.

3.0 Risks

Unauthorised remote access
Unauthorised local access
Accidental loss
Systems failure
Physical loss by fire, flood or theft

4.0 System Specific Security Policies

4.1 Third Party Managed Remote Servers

All remote servers to be managed by third parties who have been vetted by Digital Spotlight Limited staff, and shall provide a copy of their Information Security Policy. The 3rd Party Managed Remote Server Solutions shall be vetted for security, service reliability, disaster recovery, solution fitness of purpose and support response.
Servers to be maintained with the latest security patches.
Administrative access to servers, both local and remote, by approved staff only.

4.2 Local Servers & Backup Devices

Servers & backup Devices to be maintained with the latest security patches.
Access to Local Servers & Backup Devices by Digital Spotlight Limited staff only.
Regular backups of project code and assets, test data, Personnel data, financial data and security data to be taken as and when required.
Backups to be maintained both on and off site.
Local Servers and on site Backup Devices to be located in locked fire resistant cabinets.
Offsite Backup Devices to be held at a secure location.
Personnel data, financial data and security data to be password protected.

4.3 Desktop Computers

Desktop Computers to be maintained with the latest security patches.
Access to Desktop Computers, by Digital Spotlight Limited staff only.
Regular backups of project code and assets, test data, Personnel data, financial data and security data to be taken as and when required.
Desktop Computers to be located at a secure location.
Personnel data, financial data and security data to be password protected.

4.4 Mobile Devices (including Laptops, Tablets & Mobile Phones)
Mobile Devices to be maintained with the latest security patches.
4.4.1 *Onsite (secure location)*
Access to Mobile Devices on site, by Digital Spotlight Limited staff only.
4.4.2 *Offsite*
Prior to a Mobile Device leaving secure location, any Sensitive Information must either be removed or password protected. Those individuals removing any company Mobile Device from a secure location, to be additionally vigilant until device returns to a secure location.
To minimize risk, ensure that only required data is on any Mobile Device prior to move from a secure location.

4.5 Paper Documents
Paper Documents to be located at a secure location.
Access to Paper Documents by Digital Spotlight Limited staff only.
Paper Documents to be stored in cabinets.

5.0 Reporting of Security Incidents & Actions

A Security Incident is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of any Sensitive information as described in 2.0 or any breach of any System Specific Security Policy in 4.0.
All Security Incidents shall immediately be reported to management and appropriate action taken. Any Security Incidents involving client Sensitive information shall also be reported, along with any corrective action at the earliest opportunity to that client.

6.0 Policy Review

This policy shall be reviewed by senior management at Digital Spotlight Limited every 12 months.