Reviewed 5th January 2020
By Holly Roberts

Information Security Policy

Statement

The security and protection of information is fundamental to the effective and efficient working of the company and the maintenance of confidentiality. This policy provides a framework within which allows us to handle information and data in the most secure way, given the demands of the company. Security is everyone's responsibility and all personnel working in the company must make every effort to comply with this policy.

Scope of policy

The need

To meet legal and professional requirements to our client, the company must use cost effective security measures to safeguard its information resources. This company security policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The policy

The policy of the company is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised best practice

Applicability

The policy shall apply to all partners and staff of the company and any other sub-contractors using the IT resources of the company.

Implementation

The requirements of the policy shall be implemented by all partners, staff and any other sub-contractors using the company's IT resources including the creation of new resources both internally and for clients. Any team member noting any area of conflict between this Policy and any other company Policy must bring it to the attention of the Holly Roberts – Head of Operations as Security Officer of the company, immediately for conflict resolution. Holly Roberts (Head of Operations) will in any case be responsible for the routine periodic review of the Policy. Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the Policy. Compliance with the Policy is the duty of all partners and staff. In serious cases, failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence. Staff have an obligation to report suspected breaches of the Policy immediately to Holly Roberts in the case of a breach or suspected breach that could affect the security of Owl Live.

Information resources

The Policy applies to all information whether spoken, written, printed or computer-based, which is owned, held in the custody of, or used by the company, including telecoms and mobile phones
The Policy also applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

Objectives of the policy

The objectives of the Policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss.
- Information is authentic.
- Information and equipment are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented.
- Audit records on the use of information are created and maintained as necessary.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

Legal obligations

General
The company accepts its obligations to comply with the laws of the United Kingdom and other territories where relevant (e.g. EU legislation). All staff and associated parties must be aware that there are legal requirements relating to information that must be met. The principles of these are detailed below.

Data protection act
Information held electronically that relates to individuals is subject to the Data Protection Act 1998, that places obligations on those who record and use personal data and the organisation for which the work.
Antony Greenberg – Managing Director (Holly Roberts deputising) is appointed Data Protection officer and is responsible for registration matters with the Office of the Data Protection Registrar, application of the Data Protection Principles and the briefing of all Data Users within the team.

Software copyright
Software is protected by the Copyright, Designs and Patents Act 1988, which state that 'the owner of the copyright has the exclusive right to copy the work'. It is illegal to make copies of software without the owner's permission. Penalties include unlimited fines and up to two year in prison.

Computer misuse act
The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer. The offences are:

- Unauthorised Access to Computer Material
- Unauthorised Access with intent to commit or facilitate the commission of further offences
- Unauthorised Modification of Computer Material

Key security controls

Personal security
Holly Roberts and Antony Greenberg will ensure that all contracts of employment for permanent staff and contracts for 3rd parties include a 'non-disclosure' clause. Holly Roberts will ensure that security responsibilities are allocated to staff and written into job specifications and terms of reference. Security education and training will be provided to all staff as appropriate to their assessed needs.

Physical security control

1. Principle
Resources associated with information processing, such as offices, computer equipment, communications media and paper-based records shall be protected from unauthorised access, misuse, damage or theft.
2. Access
The non-public areas of the company premises are designated a secure area. Visitors are to be escorted at all times.
3. Equipment Security
All hardware and software assets held by the company are to be held against a hardware register and be uniquely marked as being the property of the company. No alteration to the hardware configuration of the system may take place without the permission of Holly Roberts. On-going maintenance arrangements have been agreed with IT Farm (Company's IT Consultants). Only approved systems engineers and the relevant staff members will be allowed access to make hardware or software changes and such access is recorded. No remote diagnosis or repair services are permitted unless

they are through IT Farm or approved by Holly Roberts. All such diagnosis and repair is to be recorded.

Computer hard discs are not to be removed from the company premises without the written permission of Holly Roberts or Antony Greenberg. The disposal of any storage media is subject to specific security control. Simple deletion of files is not adequate and the advice of IT Farm and Holly Roberts is to be sought before any disposal.

External Data e.g. that on sites created for clients is held on servers provided is UK Fast. Their data centres are ISO27001 accredited and secure to UK government IL4 standards and have been audited by Holly Roberts so are approved for us.

Internal security control

1. Principles

All information shall have an official owner who will be fully accountable for its protection and who will be responsible for:

- Assigning a security classification where appropriate.
- Defining who is authorised to access the information on a need-to-know basis.
- Assessing the risks to the security of the information and the impact of its loss, for both short and long periods.
- Employing suitable measures to reduce risks.
- Ensuring that equipment is only utilised for company business.
- Ensuring that information is authentic, correct, complete and auditable.
- Ensuring that information is backed up regularly and at a frequency commensurate with its usage.
- Safeguarding and retaining all company records.
- Ensuring that information exchange with external organisations does not compromise the confidentiality of sensitive information, nor does it increase the risk of data corruption.

2. Security Incidents and Reporting

A security incident is defined as any event that could result or has resulted in:

- The disclosure of confidential information to any unauthorised individual.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.

An adverse impact, for example:

- Embarrassment to the company, its clients or servants.
- Threat to personal safety or privacy.
- Legal obligation or penalty.
- Financial loss.
- Disruption of activities.

All incidents or information indicating a suspected or actual breach of security must be reported immediately to Holly Roberts. The types of incidents that can result in a breach of security are many and varied. Their severity will depend upon a myriad of factors but the majority will be innocent and unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security and awareness throughout the company.

Any unusual incident must be reported to Holly Roberts who will maintain a record of incidents. If an incident is considered to be significant, Antony Greenberg is to be informed.
Any member of staff reporting a breach of security will have unhindered access to Holly Roberts. If that member believes the breach is as a result of an action or negligence on the part of Holly Roberts then the member will have access direct to Antony Greenberg.

Please refer to the Security Incidents Policy for full details

3. Virus Protection

A computer virus is a computer program, which ‘infects’ (modifies or attaches itself to) other computer programs. It then replicates itself and when a set of conditions arises it performs its intended function. This can range from a silly message to the destruction of the complete data holding of a system. A constantly running anti-virus software package (ESET) has been provided and set to auto update latest virus signatures. This does not absolve users from specifically checking any externally sourced discs or emails for viruses before downloading any data or application.

4. Passwords

Passwords are an effective security measure only if they are properly constructed and kept secret. Partners and staff will follow the following routines for password management. All users should have an individual user name for logon. All passwords are to be changed on a regular basis through system forced password changes (every 45 days at minimum). Additionally, users are to change their password at any time that they feel their password has been compromised. Passwords should be given values that are not associated with personal characteristics, (e.g. children’s names, telephone numbers, car registration numbers etc.) Simple and obvious strings of characters and numbers should not be used. A combination of alphabetic, numeric, upper and lower case and system characters are to be used and have a minimum of 8 characters. Passwords should not be written down except as possible reference by Holly Roberts under strict security control. Passwords are not to be revealed to or shared with other users, breach of this will be deemed as gross misconduct. All users will be automatically made to change their passwords every 45 days as per the company policy.

5. System Access Controls

No terminal, PC, Laptops or mobile phone is to be left logged on and unattended. Users leaving their workstation are to log off the system, or change user, to prevent unauthorised access.

6. Creation of Digital Content

Owl Live from time to time will create digital content for our clients. It is imperative that any and all digital content meets the conditions of this policy. All content must go through rigorous testing including penetration testing, SSL labs, load testing and ensure DDA compliance. Any online content must be hosted by UK Fast as our approved contractor. All websites must have SSL certificate applied with SHA-256 and RSA Encryption. All data held must ensure full compliance the our data protection policies

7. Housekeeping

Data backup of the complete system will be effected twice daily by IT Farm. All company documents / data must be saved on the shared server to ensure minimum risk of lost data. All backup data will be accorded the same level of security as live data and held separately at an off-site secure location. Removable storage media such as DVDs, CDs, and USB sticks should be cleared of any data (if sensitive / confidential this must be passed to Holly Roberts for effective removal) and stored in a secure environment and encrypted when not in use. All software in use by the company must be licensed and networked applications may be subject to a limited number of users. Holly Roberts is to ensure that software is correctly used against licences held. Software is not to be loaded onto any system or PC without the express authority of Holly Roberts and security controls on then local machines will not allow admin access to anyone other than Holly Roberts and Antony Greenberg. This Policy is also to be reflected in employee’s terms and conditions of employment.

8. Service Continuity Planning

Disaster Recovery and Service Continuity Contingency plans are to be produced to ensure the continued fulfilment of the company mission (please refer to continuity policy).

Role of the company security officer
Holly Roberts is the nominated Security Officer for the company and shall, under the direction of Antony Greenberg, develop and manage the company security programme:

- Develop, issue and maintain the IT security strategy and Policy and agree them with Antony Greenberg
- Maintain a strategic IT Disaster Recovery & Service Continuity Plan and advise the company on its implementation.
- Create an information security awareness programme to include whole company briefings, training and education.
- Provide information security consulting support to the company.
- Investigate breaches of security and report findings and recommended action to the company.
- Implement a compliance programme to evaluate the effectiveness of the information security programme.
- Report annually to Antony Greenberg on the effectiveness of the overall information security programme.

Policy review
This Policy is to be reviewed on an annual basis by Holly Roberts to take account of changing circumstances, legislation, technology and security risks.

Associated policies:
Business Continuity Policy
Data Protection Policy & Procedures
Security Incident or Breach Policy
Data Classification Policy