Ovation
SOUND FINANCIAL MANAGEMENT

Data Security Policy

Ovation Finance Limited

December 2017

FCA number 190914

Table of Contents

Purpose of Our Data Security Policy

The main purpose of this data security policy is to inform staff and managers of their obligatory requirements for protecting technology and information assets. This policy specifies the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit our internal systems and processes for compliance with the policy.

This policy may be read in conjunction with Ovation's Business Continuity Plan, and staff policies.

What Needs Protecting?

The key assets requiring protection through a data security policy have been identified as:

1. Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, laptops, other portable devices, printers, disk drives, communication lines, terminal servers, routers.
2. Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.
3. Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.
4. People: users, administrators, hardware maintainers.
5. Documentation: on programs, hardware, systems, local administrative procedures.
6. Supplies: paper, forms, ribbons, magnetic media.

For convenience we have broken these assets down into specific business areas which we need to protect – Physical Security, IT Security, and Intellectual Property.

Physical Security

These are the means by which we ensure that premises and documents are kept secure from unauthorised access.

Protecting the Building

The building is protected from unauthorised access by:

1. Door entry codes for the front and car park entrance
2. Locked internal doors preventing access to main office and meeting room – a list of who has which keys is available
3. Security guard on site out of office hours
4. An office intercom to vet visitors
5. Staffed reception area to vet and sign in visitors

Protecting Documents in the Office

Documents are protected from unauthorised access by:

1. Locked, fireproof safe for overnight storage of client cheques.
2. Clear desk policy to avoid documents being left on desks and on view overnight.
3. Confidential paperwork is placed in secure containers and shredded monthly
4. All documents are scanned and shredded within one day of receipt.

Use of External Third Parties / Outsourcing

If any IT administration processes such as back up of data, support of the various IT systems and data storage e.g. via the cloud are outsourced, the specific procedures will be followed and due diligence on the firms concerned will be carried out.

Other third parties e.g. cleaners or cleaning companies whose staff can access client data will also be subject to the same due diligence.

Our procedures will include:

1. Understand the third party's data security procedures.
2. Carry out appropriate due diligence on those third parties, including their data security arrangements and staff recruitment policies.
3. Consider whether we should allow third parties unsupervised access to the office or records.

IT Security

These are the means by which we ensure that any electronically stored information is kept secure from unauthorised access.

Protecting Infrastructure and Hardware

Servers, personal computers, laptops and other portable devices are protected by external attack from unauthorised access, viruses and trojan horses by:

1. Hard password policy on all servers, personal computers, laptops and other portable devices. All passwords must be at least seven characters long and include one capital letter and one number. Users are forced to change password every calendar month.
2. Ovation's Anti-virus is managed by Alliance Systems Limited and is regularly updated and applied to Ovation's systems
3. All incoming emails are scanned by an external agency before they are delivered onto the network.
4. All incoming emails are filtered for spam and quarantined for checking before they are delivered onto the network.
5. Wireless network is secured via WPA encryption.
6. The Ovation Staff Policies prohibit staff from opening emails or attachments from unknown sources
7. Network and individual computer administration rights are controlled by virtue of the individual role held and are granted only to senior staff.
8. Staff may not undertake Ovation work on personal computers.

Use of Personal Devices

Staff may use personal devices (mobile devices only) for work but only where this has been agreed in advance and the following points have been considered:

1. Being clear with staff about which types of personal data may be processed on personal devices and which may not.
2. Using a strong password to secure their devices.
3. Enabling encryption to store data on the device securely.
4. Ensuring that access to the device is locked or data automatically deleted if an incorrect password is input too many times.
5. Using public cloud-based sharing and public backup services, which you have not fully assessed, with extreme caution, if at all.
6. Registering devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft.

Disposal of Hardware

Consideration is given to the disposal of computers, laptops, other portable devices, memory sticks, disks etc.

1. If a third party is used for the disposal of data, the firm will satisfy itself with their data security and staff vetting arrangements.
2. Disposal of a computer (or other equipment which potentially stores client records e.g. some photocopier/scanner equipment) - the hard drive will be wiped with specialist

software or removed and destroyed sufficiently so that information cannot be accessed by an authorised person.

Working from Home

Developments in technology means it is more and more possible for staff to work from home. This will depend on an individual's role and will need to be agreed with line management in advance.

Where home working is agreed, there are several areas that need to be considered in relation to data security. These considerations apply to all work-related documents i.e. paper-based and electronic records.

Working on work related documents at home will always involve an element of risk so careful thought is needed as to what data needs to be accessed or taken home. As referred to earlier, this is also likely to depend on the individual's role.

The measures needing to be taken when staff are working from home will in many ways mirror many of the precautions taken for office-based staff. Reference should therefore be made to other sections of this document – as well as considering the areas below.

Home computing

- Staff should work directly from/to the appropriate business server using remote access facilities provided where possible. This reduces the need to take home electronic information or to store it there, addresses business continuity concerns and limits the additional security measures needing to be taken regarding electronic information.
- If staff use a business laptop, this should not be used to store the only copy of business and/or client records as it is more vulnerable to loss or theft. Plan to back up information that is stored on a laptop and store this on your business network.
- All business computers, laptops and similar electronic equipment and applications will be kept up to date with virus protection software and security patches.
- Only work email addresses and accounts will be used by staff when dealing with work related business.

Physical security

- Where paper-based records need to be taken home, where possible, a copy rather than the original file / documents should be taken. Where this is not practical, and the original file / document needs to be taken, a record of this should be made on the back-office system in some way so that colleagues are aware of where the file / documents are.
- Any work-related records should be updated as soon as possible with any work that is undertaken at home.
- When staff work at home, security should be of the same standard as that which is provided in the office.
- Ideally, the work area at home should be in a separate location to general 'living' areas. This location should not be able to be easily seen or accessed by people outside the home. For example, do not situate your work area or computer station next to a ground floor window.
- Care should be taken to ensure that work related information is not left where others at home can see it.
- Paper documents, files and portable media devices should be stored in a lockable cabinet which is locked when not in use.
- Care needs to be taken when transporting work related records to or from home;
    - If traveling by public transport, all work documents should be stored or held securely. Hold onto bags or laptops rather than placing them on luggage racks. Keep smaller

storage media, such as portable drives, in secure compartments of bags, rather than in a jacket pocket.

- If traveling by car, work related documents and laptops should be locked securely in the boot. Do not leave these in plain sight.

- Work related records should be disposed of securely and appropriately. For example, documents you no longer need, should not be disposed of in general waste or recycling bins; a shredder should be used or alternatively, the documents be disposed of using the normal confidential waste facilities at the office.

Protecting Intellectual Property

These are the additional means by which we ensure that our intellectual property, and the goodwill of the business, is kept secure from unauthorised access.

Staff

Staff are made aware of their obligations through:

1. Ovation staff policies/employment contract/self-employed contract.
2. Induction process which covers this data security policy.
3. Annual training on data security.
4. Updates to changes on data security policy.
5. Annual test on data protection.

Use of all business equipment is governed by the Staff Handbook which ensures that:

1. All business equipment is logged against staff member.
2. Laptops must be locked away and not left in insecure locations/
3. Staff may not undertake work on personal computers.
4. Staff may not email work to personal email accounts.

Staff Leavers

The business is protected from employed and self-employed staff who leave as:

1. All Ovation property including devices, keys and business cards must be returned to the office on leaving.
2. Staff can be placed on 'gardening leave' on resignation.
3. Restrictive covenants are in place to prevent solicitation of clients after leaving.
4. Staff Contract and Policies makes explicit reference to confidential information and ownership of client data.

Access Rights

Access rights to information on the network and emails are controlled using an access policy which ensures that:

1. Access is granted to data only where required and where approved by the IT decision group.
2. Temporary access to data must also be time bound, and privileges revoked after that date or an extension expressly granted by the IT decision group.
3. A register is maintained listing what access rights have been given and to which staff. This is maintained and updated by Elizabeth Thomas and Alliance Systems Limited.

Requests for and Exchange of Information

Telephone

All inbound calls from clients for the following are subject to verification using the Client Authentication Form at Appendix 1.

1. Change to any contact details
2. Request for the movement of client funds
3. Request for any values or policy information
4. Any other suspicious requests or requests for information which might reasonably be used for fraud

Email

All email requests from clients for the following, are subject to verification by contacting the client by telephone and verifying the request using the Client Authentication Form at Appendix 1.

1. Change to any contact details
2. Request for the movement of client funds
3. Request for any values or policy information
4. Any other suspicious requests or requests for information which might reasonably be used for fraud

Letter

All requests by letter from clients for the following, are subject to verification by contacting the client by telephone and verifying the request using the Client Authentication Form at Appendix 1.

1. Change to any contact details
2. Request for the movement of client funds
3. Request for any values or policy information
4. Any other suspicious requests or requests for information which might reasonably be used for fraud

All correspondence sent back to the client containing original client documents, must be sent using registered delivery.

Request for Information under the Data Protection Act

Any individual requesting information held on them under the Data Protection Act has a right to such information, subject to certain limitations.

All such requests should be forwarded to Elizabeth Thomas who is responsible for the processing of such requests. Under no circumstances should staff provide this information without reference to Elizabeth.

Data Security Violations/Data Compromise Reporting Policy

All Ovation staff are under an obligation to report any incident which you may feel violates the data security of the business by informing Elizabeth Thomas by email or in person. All violations are recorded in the Data Security Violations Register on sharepoint.

Equally all staff are aware of the need to report any data compromise incidents. These can include:

1. Loss of laptop or another portable device.
2. Loss of client data either in paper form or electronic.
3. Unauthorised persons in back office area where data stored.
4. Client information passed onto unauthorised third party.

All incidents should be reported immediately to Elizabeth Thomas and these will be entered up on a Data Compromise Register on sharepoint. Ovation will take steps to provide remedial action as appropriate, e.g. informing the FCA, the police and other regulatory or governing body and provide staff training.

Audits

Compliance with this policy is audited on an annual basis by Elizabeth Thomas. The results are detailed on sharepoint.

Appointed Representatives

All appointed representatives understand that the Ovation is responsible for ensuring that adequate systems and controls are in place at any premises the appointed representatives are based in. This includes proper data security procedures.

All appointed representatives must hold a valid Data Protection Act Licence or be listed on our entry.

Checks will be made annually to ensure that the appointed representatives have adequate safeguards in place to protect client data as listed in the above sections. Compliance with this policy is audited by Elizabeth Thomas. The results are detailed in the Security Audit Register on Sharepoint.

Appendix 1 - Client Authentication Form

Note to confirm the caller they will need to provide the following information.

- A minimum of 5 items of information must be confirmed (3 personal details, 2 financial details);
- If the caller cannot verify 5 items of information, then:
- ask the caller what information they are calling for and;
- Advise the caller that the information will be posted to the home address that is stored on the client file.

Date	Time	Reason for Call			
Tier 1 authentication (client must provide all 3 items)					Yes / No
Full name					
Date of birth					
Full address and postcode					
Tier 2 authentication (client must provide a minimum of 2 items)		Yes / No			Yes / No
Name of bank/building society			Name of protection provider		
National Insurance number			Sum assured (life assurance)		
Name and address of GP			Name of pension provider		
Mobile phone number			Pension contribution		
Authentication outcome		Yes / No	Next Steps		Yes / No
Confirmed			Information provided over the phone		
Failed			Information to be sent in the post to address on client file		
Additional Comments					

Appendix 2 – Data Security Violations Register

Date Violation Identified	How Violation was Discovered	Date of Actual Violation	Description of Violation	Date of Notification to Regulator	Any Remedial Action

Appendix 3 – Security Audit Register

Date of Audit	Area Audited	Name of Auditor	Results of Audit	Any Remedial Action