Data Security Policy

Prepared by Caroline Davidson (Secretary)

XX March 2016

Policy Scope

This policy applies to

- Executive Committee members of Visit USA (Organisation) Australia (**VUSA / the Organisation**)
- Committee Members
- Secretariat
- Other contractors, suppliers, volunteers and anyone working on behalf of the Organisation e.g. PR contractor

It applies to all data the organisation holds relating to identifiable individuals e.g. Members, agents, media etc including

- Names
- Email and postal address
- Phone numbers
- Other information

Policy protection objectives

To protect the organisation against

- Breaches of confidentiality;
- Failing to offer choice of individuals/members as to how their data is used by the organisation; and

- Reputational damage to the organisation (e.g. in event of hackers gaining access to private info etc.).

Responsibilities (these to be determined and added)

Everyone who works for or with the Organisation is responsible for ensuring data is collected, stored and handled appropriately.

- Executive Committee
- Committee
- Secretariat
- IT Consultant/contractor
- PR Contractor

General Guidelines

- Access to VUSA data should be restricted to those who are currentExecutive Committee Members or employees /contractors of the organisation;
- Data should not be shared informally;
- All Committee Members and Employees should be made aware of policies and procedures relating to data security;
- All Committee Members and mployees / contractors should keep data secure by taking sensible precautions and following guidelines below;
- In particular strong passwords must be used and never shared;
- Personal information should not be disclosed to unauthorised people either externally or within the organisation; and
- Data should regularly be reviewed and updated or if no longer required it should be deleted or disposed of.

Data Storage

If data is on paper it should be stored securely where unauthorised people cannot view it. This also applies to electronically stored data which has been printed which should be shredded when no longer required.

When data is stored electronically it should be protected from unauthorised access, accidental deletion and hacking attempts.

Strong passwords must be used, changed regularly and never shared.

If data is stored on removable media such as a usb etc. they should be stored and locked away securely when not in use.

Data should be only stored on designated servers, and should only be uploaded to an approved cloud computing services.

Server containing personal data should be sited in a secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the organisation's standard backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to VUSA unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft, therefore:

- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.;
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts; and
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

VUSA strictly adheres to the Australian Privacy Principles, these principles cover:

* the open and transparent management of personal information including having a privacy policy

an individual having the option of transacting anonymously or using a pseudonym where practicable

the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection

how personal information can be used and disclosed (including overseas)

maintaining the quality of personal information

keeping personal information secure

right for individuals to access and correct their personal information

Data accuracy

The law requires VUSA to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort VUSA should put into ensuring its accuracy.

It is the responsibility of all staff (VUSA Members/employees/contractors) who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets;
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a member's details when they call;
- VUSA will make it easy for data subjects to update the information VUSA holds about them. For instance, via the organisation's website;
- Data should be updated as inaccuracies are discovered. For instance, if a Member can no longer be reached on their stored telephone number, it should be removed from the database; and
- It is the Secretariat's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by VUSA are entitled to

- Ask what information the organisation holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the organisation is meeting its data protection obligations

If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [email address]. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law agencies without the consent of the data subject.

Under these circumstances, VUSA will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Exec Committee and from the organisation's legal advisers where necessary.

Providing information

VUSA aims to ensure that individuals are aware that their data is being processed, and that they understand

- How the data is being used; and
- How to exercise their rights.

To these ends, the organisation has a Privacy Statement, setting out how data relating to individuals is used by the organisation. [This is available on request. A version of this statement is also available on the organisation's website.]

AND OPTIONAL INCLUSIONS AS CONSIDERED RELEVANT FROM THE FOLLOWING:

5 Step Data Security Plan for Small Business (adapted from US Security consulting business blog post: http://www.wilkins-consulting.com/small-biz-security-plan.html)

Step 1 - Asset Identification/Classification and Risk Assessment
Identify Information Assets
The first step is to identify our information assets. Examples would be computers, phones, servers, fax machines, paper, flash drives/removable media, etc.

A good rule of thumb is that if it contains Member or VUSA business proprietary data, then it should be considered an information asset. Once we have identified our information assets, then these will need to be tagged and inventoried. It can be as simple as using the serial number and description of the asset and inventorying it in an excel spreadsheet to bar coding and tagging each asset and inventorying in a database. In addition assign an Exec Committee person responsible for every asset.

D13

	A	B	C	D	E
1		High	Medium	Low	
2	Laptop (medium confidential data)		x		
3	Desktop (abundant confidential data)	x			
4	Server (all your confidential data)	x			
5	Desk phone (minimal confidential data)			x	
6					
7					

Once we have identified the assets, we need to classify them in a level of importance. Keep the classification system simple with High, Medium, and Low. Assets that contain Member information or proprietary organisation information would obviously have the highest level of importance while assets that contain organisation marketing information for example might be given a low classification.
Risk Assessment of Information Assets
The final step would be to develop a risk assessment either for each asset class (eg. computers, phones, paper, etc) or for each asset classification (high, medium, low), and determine the risks you are willing to accept. You first need to determine the threat, vulnerability, and impact (TVI) on each individual asset or class of asset. The threat to the asset would list the different reasons/methods of how the asset could fail. The vulnerability is the situation that could lead to this failure. The impact is the influence of the effect on the integrity, confidentiality, and reasonable availability of the information asset.
EG:
Asset: Network server that contains your company data
Classification: High because it contains classified and irreplaceable date.
Threats: HDD failure, virus, theft
Vulnerability: Medium - High
Impact: Very High
Level of Risk You Accept: You would want to take enhanced security measures such as keeping it locked up, behind a network firewall, and backed up. But it may be too expensive to backup your main server with a second server for real-time redundancy. In this case, to reduce costs but still ensure a backup in case of an emergency, you might be willing to accept a little added risk by backing your server up to tape which will require a longer downtime (takes longer to restore a backup tape) if the server was damaged.

Follow these steps, and you will clearly understand your information assets and the controls you need to put in place to protect them. And as you add new assets, update your database accordingly.

Step 2 - Network and Physical Access Security Controls

Network, Computer, and Email Access Controls

- Require all employees to use password authentication to access their computers, the corporate network, and email.
- Set computer passwords to expire every 90 days.
- Use strong passwords - Minimum of 10 characters, combination of at least 3 of the following 4 (letters, numbers, and special characters, capitalized or lower-cased characters), do not use common words.
- It may be necessary to give employees different levels of access depending on the data stored on your corporate network. For example if you store personal client information (credit card, bank account, social security number, etc) on your corporate network, then you should determine which employees need access.
- Mobile computing - If you allow employees to access your corporate network via mobile access programs such as VPN, ensure that connections to your network are securely authenticated and that mobile computers are password protected. In addition consider passwords for employee mobile phones if the phones are used for company email access.

Physical Access Controls

- If you keep network servers on your company premises, then ensure they are encrypted and kept behind locked doors at a minimum. Limit employee access to servers.
- The type of corporate data you store on your company premises will have a direct impact on the type of physical access controls required. If the data is sensitive, then consider enhanced access security such as biometric, video cameras, third party security monitoring, etc. Many of these controls can be put in place rather inexpensively.
- If you host your corporate networks at a remote third party facility, keep it local if possible, and tour the remote facilities to ensure they have the proper physical and environmental protections.

Review of Access Controls

Once you have your physical and network security controls in place, it is crucial to review access controls. For example when employees leave your company, you want to ensure they no longer have access to any data. Your access control review schedule will depend on the amount of employee turnover at your company. If the turnover is more frequent, you should review access controls on a monthly basis. If it is less frequent, quarterly reviews will be more appropriate. You will want to check email, network, phone, mobile, and physical access controls. Set calendar reminders, and stick to the schedule.

Follow these steps to ensure proper network and physical security access controls in addition to setting a review schedule.

Step 3 - Network and Personal Computer Security Controls

Encryption

Encryption is probably one of the cheapest and most secure steps a small business can take. Encrypt your corporate server, work computers, laptops, flash drives, etc, and even if they are stolen, the data will still be safe from intrusion. And you can reliably encrypt media for free using programs such as DiskCryptor or TrueCrypt.

In addition if you send sensitive data via email, encrypt the emails using a program such as MessageLock or PGP email encryption.

Anti-Virus/Anti-Spyware
Make sure you have anti-virus software on all of your work computers, and keep them updated

Downloads and System Acceptance
Know the types of downloads you need to make to update and add software. In addition test new downloads and programs for system acceptance on an isolated (from your office network) system before running it across the entire organisation. Ideally run all downloads, upgrades, etc., through one person such as a network administrator or if you outsource to an IT company.

Firewall and Internet Connection
Ensure that you have your network or computers behind a firewall, and update it with security updates. In addition you should routinely (quarterly or bi-annually) scan your firewall for vulnerabilities and fix any issues.
Although I do not recommend it, if you use a wireless network in your office for your internet connection, use WPA2 encryption.

Network and Computer Backups
If you are a very small company with only a few computers, then you can easily backup to a flash drive or hard drive and take it offsite or keep it locked in a good secure (ie. bolted down) fireproof safe. In addition you should encrypt the flash drive, or any backup media for that matter, using a program like TrueCrypt. You also have the option of backing up to online sites
like Mozy or Carbonite.
No matter what type of backup you are doing, get in the habit of doing it on a regular schedule either daily, weekly, or a combo of both. If you have to do the backups manually, set up calendar reminders until it becomes a habit. Keep records of your backups. And do test restores from time-to-time to make sure there is no corruption of any kind.

Third party network security checks
In addition you should consider bringing in a third party at least once a year to check for additional network and computer vulnerabilities.
Follow these steps to ensure proper network and personal computer security controls.

Step 4 - Paper document controls
Information Classification Policy
The first step to securing your paper documents is to classify them. Keep your classification system simple, and I recommend no more than four classifications for document assets.
Examples

- **Public** - This type of information is not confidential and can be made public. Examples of this classification type are marketing materials.
- **Proprietary** - You would restrict this type of information to management-approved internal and external access. Examples of this classification type are policies and procedures. In some cases these document types may be required by clients to review the operational structure of your business.
- **Client Confidential** - Defined as information received from your customers that is proprietary and confidential. An example of this type of information is customer bank account info. This information type is restricted to management-approved internal access only.
- **Company Confidential** - This is confidential information that your company uses to conduct business. Examples of this type of classification are financial documents or personal

employee information. You would tightly restrict access to this information within your company only.

Once you have classified your documents, consider setting up document templates and incorporate the document classifications which enable you to correctly monitor the dissemination of your documents.

Shred Documents

If any sensitive documents are marked as trash, then shred them. Keep documents that need to be shredded locked up until you shred them. This would also be part of your clean desk policy as you would not leave sensitive documents unmonitored on employee desks.

Filing Cabinets

Keep filing cabinets locked at all times, and if feasible keep them behind locked doors. Keep keys locked in a single location with limited access.

Follow these steps to ensure proper paper document security controls.

Step 5 - General security controls

Employee Background Checks and Training for new Hires

Run criminal history and credit background checks on your employees especially for those that will be handling sensitive information. In addition conduct training for new hires to make them familiar with your security policies and procedures.

Third Party Review

Depending on the sensitivity of the data stored at your office location, consider a third party review at least yearly. You could conduct a review of your complete security procedures in addition to network and physical security access.

Visitor Policy

If you have a constant flow of visitors to your office, consider a visitor policy. There are several options for a visitor policy, once again depending on the sensitivity the data stored in your office. Options include sign-in/sign-out sheet, ID check, name tags, and designated areas that are off limits to visitors without a company escort.

Incident Management System

Keep a system for logging any type of security incidents, how you corrected the issue, and how you will prevent it in the future. This can be as simple as an excel spreadsheet up to a tracking database.

Emergency Response Plan

Depending on the size of your company and the sensitivity of the customer data you store, the emergency response plan would be a key cornerstone of a business continuity plan (BCP). Smaller companies can almost use their emergency response plan as a BCP. Keep the emergency response plan simple and direct, and key elements to be included are as follows:

- A plan to determine who is in charge and who is responsible for each action covered below.
- Key personnel contact information - Obviously for contact but also to set in motion pre-assigned duties and responsibilities.
- Key contact information for service providers such as third party network administrators, security monitoring, phone, internet, etc.
- Key contact information for your local police in addition to your legal representation
- Backup communications plan

The goal of your emergency response plan and the 5 Step Data Security plan in general is to ensure all preparations have been made to minimize the severity of any security incidents or emergencies in addition to personal danger and physical property damage. In addition you want to ensure you have an effective communication plan to initiate recovery operations and to get your business up and running as soon as possible if there is any down-time.