OCData Information Security Policy

Table of Contents

Terms of Reference

For brevity and ease of updating during the review process, the following terms are used in substitution throughout this document.

The Company	OCData
Dir	Director – Greg Smith
IM	Imagine Multimedia – Managing Director - Graham Hett
NDB Scheme (Australian Government)	Notifiable Data Breaches Scheme

Introduction

The purpose of this IT security policy is to:

- Reduce the risk of IT problems
- Plan for problems and deal with them when they happen
- Keep working if something does go wrong
- Protect company, client and employee data
- Keep valuable company information, such as plans and designs, confidential
- Meet our legal obligations under the Privacy Act
- Meet our professional obligations towards our clients and customers

The company strives to achieve a prevention outlook, rather than react and resolve, which can be expensive and time-consuming.

Responsibilities

- Greg Smith is the director with overall responsibility for IT security strategy
- Greg Smith has day-to-day operational responsibility for implementing this policy
- Imagine Multimedia is the IT partner organisation we use to help with our planning and support.

Review History

This policy is to be reviewed on a 6-monthly frequency.

Version & Date	**Comments**	**GM Approval**	**IM Agreement**
V0 – 19/03/2021	Create policy	19/03/21	
V1 – 3/6/19	Initial review after release		

Information Classification

The Company will only classify information which is necessary for the completion of work. The Company will also limit access to personal data to only those that need it for processing. Information is classified into different categories so that staff can ensure that it is protected properly and that security resources are allocated appropriately:

- **Unclassified.** This is information that can be made public without any implications for the company, such as information that is already in the public domain.
- **Employee confidential**. This includes information such as medical records, pay and so on.
- **Company confidential.** Such as contracts, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.
- **Client confidential**. This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information etc.

Information that the company keeps has been categorised as follows:

Type of information	**Systems involved**	**Classification level**
School student records	SIS	Client confidential
Employee records	SIS	Client confidential
IT infrastructure build docs	Protected File Shares	Company confidential
Client project information	Protected File Shares	Client confidential
Client quotes and proposals	KIM Software	Company confidential
Tender documents	Protected File Shares	Company confidential

The deliberate or accidental disclosure of any confidential information has the potential to harm the business. This policy is designed to minimise that risk.

It should be assumed that all information is confidential unless the Dir has specifically noted that it is not and act accordingly.

Access Controls

Internally, as far as possible, the company operates on a ‘need to share’ rather than a ‘need to know’ basis with respect to company confidential information. This means that the bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

As for client information, the company operates in compliance with the Privacy Act and understands that it is the right of data subjects to obtain confirmation as to whether the company is processing their data, where it is being processed and for what purpose. Further, the company shall provide, upon request, a copy of their personal data, in an electronic format.

However, in general, to protect confidential information the company implements the following access controls:

- Company confidential.
- Client confidential.
- In addition, admin privileges to company systems will be restricted to specific, authorised individuals for the proper performance of their duties as follows: [see table below].

Security Software

To protect our data, systems, users and customers we use the following systems:
- Laptop and desktop anti-malware [Windows defender]
- Server anti-malware [Clamav]
- Desktop firewall [Windows firewall]

Staff Onboarding/Exit

When a new employee joins the company, we will add them to the following systems:

Data Type	Role	Access
Corporate Data	Director	Full
Corporate Data	Programmer	None
Corporate Data	Exec Assistant	Partial
User Data	Director	Full
User Data	Programmer	Full
User Data	Exec Assistant	Full

Access to corporate data, and user data.

The Company will provide training to new staff and support for existing staff to implement this policy. This includes:

- An initial introduction to IT security, covering the risks, basic security measures, company policies and where to get help
- Training on how to use company systems and security software properly
- On request, a security health check on their computer, tablet or phone

When people leave a project or leave the company, their access privileges to company systems will be promptly revoked.

Staff Responsibilities

Effective security is a team effort requiring the participation and support of every employee and associate. It is your responsibility to know and follow these guidelines.

You are personally responsible for the secure handling of confidential information that is entrusted to you. You may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to your supervisor.

Protection of Devices

It is also your responsibility to use your devices (computer, phone, tablet etc.) in a secure way. However, we will provide training and support to enable you to do so (see below). At a minimum:

- Remove software that you do not use or need from your computer
- Update your operating system and applications regularly
- Keep your computer firewall switched on
- For Windows users, make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date. For Mac users, consider getting anti-malware software.
- Store files in official company storage locations so that it is backed up properly and available in an emergency.
- Switch on whole disk encryption
- Understand the privacy and security settings on your phone and social media accounts
- Don’t use an administrator account on your computer for everyday use
- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in.

Password Guidelines

- Change default passwords and PINs on computers, phones and all network devices
- Consider using password management software
- Don’t share your password with other people or disclose it to anyone else
- Don’t write down PINs and passwords next to computers and phones
- Use strong passwords
- Change them regularly
- Don’t use the same password for multiple critical systems

General Conduct

While technology can prevent many security incidents, your actions and habits are also important. With this in mind:

- Take time to learn about IT security and keep yourself informed.
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender.
- Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee, client or company confidential information. Fraudsters and hackers can be extremely persuasive and manipulative.
- Be wary of fake websites and phishing emails. Don’t click on links in emails or social media. Don’t disclose passwords and other confidential information unless you are sure you are on a legitimate website.
- Use social media, including personal blogs, in a professional and responsible way, without violating company policies or disclosing confidential information.

- Take particular care of your computer and mobile devices when you are away from home or out of the office.
- If you leave the company, you will return any company property, transfer any company work-related files back to the company and delete all confidential information from your systems as soon as is practicable.
- Where confidential information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and shredded when no longer required.

The following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

- Anything that contradicts our equality and diversity policy, including harassment.
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of confidential information at any time.

Backup and Disaster Recovery

This is how the backup and disaster recovery of business-critical systems is setup:

Automatic daily backup using Windows Backup software to RAID 5 redundant QNAP NAS device.

This is how we will respond to potential interruptions to our business:

- Following the Australian Cyber Security Centre guidelines for small business

The contingency plans are to be tested at least once a year.

We will respond to IT security issues by contacting our third party security adviser:

- Malware infection detected by scanners
- Ransomware
- System failure
- Attempted social engineering
- Data loss or theft

Under the NDB scheme, where a data breach is likely to result in ‘serious harm’ we must notify the customers and data controllers ‘without undue delay’. We will ensure we inform them within 72 hours.