northstar
design // print // promote
EST 1991

# IT & SECURITY
# POLICY STATEMENT

## Introduction

## Responsibilities

IT security problems can be expensive and time-consuming to resolve. Prevention is much better than cure.

- Gerard Lamle (senior Partner) is the person with overall responsibility for IT security strategy.
- Gerard Lamle  has day-to-day operational responsibility for implementing this policy.
- LMG Nertworks is the IT partner organisation we use to help with our planning and support.

## Review process

We will review this policy  annually.

In the meantime, if you have any questions, suggestions or feedback, please contact Gerard Lamle, ged@northstardesign.co.uk

We will only classify information which is necessary for the completion of our duties. We will also limit access to personal data to only those that need it for processing. We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources 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.

We have categorised the information we keep as follows:

Information classification

| Type of information | Systems involved | Classification level |
|---|---|---|
| e.g. customer records | e.g. Salesforce CRM | e.g. 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.

We do not protectively mark documents and systems. Therefore, you should assume information is confidential unless you are sure it is not and act accordingly.]

For client information, we operate in compliance with the GDPR 'Right to Access'. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose. Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format.

We also allow data subjects to transmit their own personal data to another controller.

However, in general, to protect confidential information we implement the following access controls:

• Company confidential - Accessed via password protected CRM system and Flyerlink job management system. Staff are given certain level of access to information

• Client confidential - Held in password protected folders on shared disk. Access only by Senior partner/director

• Employee confidential. Held in password protected folders on shared disk. Access only by Senior partner/director

### Access controls

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

To protect our data, systems, users and customers we use the following systems:

- Cloud-hosted email spam, malware and content filtering - Through our IT Company Microsoft 365
- Email archiving and continuity - Through our IT Company Microsoft 365
- Website malware and vulnerability scanning - Word fence & Sucurri

### Security software

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

• Flight CRM - access is granted to appropriate level

• Flyerlink - access is granted to appropriate level

### Employees joining and leaving

We 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
- Each employee will complete the National Archives 'Responsible for Information' training course (approximately 75 minutes)
- 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, we will promptly revoke their access privileges to company systems.

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 Gerard Lamle.

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
- 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
- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers.
- 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.

## Your responsibilities

Protecting your own device(s)

- 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

## Password guidelines

Be alert to other security risks. 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. Get Safe Online is a good source for general awareness
- 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, disaster recovery and continuity**

This is how we backup our business-critical systems.

- All work is stored on the company Cloud system which is backed up
- Additional backups are carried out via the time machine software
- All job based data held on Flyerlink and Flight CRM is backed up by the host supplier.

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

• [FOR EACH ITEM INCLUDE: WHO TO ALERT, INITIAL RESPONSE, RECOVERY ACTION STEPS, SOURCES OF SUPPORT AND ADVICE]

• Severe transport disruption - Gerard lamle

• Unable to access office because of flood, fire, civil disorder, terrorist incident etc. - Gerard Lamle

• Loss of internet and/or phone connection - LMG Networks (IT supplier)

• Loss or theft of critical systems - Gerard Lamle

We will test these contingency plans at least once a year.

Under the GDPR, where a data breach is likely to result in a 'risk for the rights and freedoms of individuals' we must notify the customers and data controllers 'without undue delay'. We will ensure we inform them within 72 hours.

Updated Jan 2022