Information Security Policy - Digicore Limited

1. Introduction

As a modern, forward-looking business, Digicore Ltd recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

To provide such a level of continuous operation, Digicore Ltd has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

The impact of an information security incident will obviously depend upon its nature and a comprehensive risk assessment is maintained to assess and mitigate those risks that can be reasonably identified.

In general terms the potential impact of an incident or breach will be shown in one or more of the following key business areas:

- Loss of sales revenue
- Risk to life on health and safety grounds
- Loss of reputation/customer confidence
- Inability to meet legal obligations
- Breach of contractual obligations
- Loss of business opportunity

This information security policy forms a key part of our set of controls to ensure that our information is protected effectively and that we can meet our obligations to customers, shareholders, employees and suppliers.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to customers. If any employee is found to have breached this policy, they will be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice in the first instance from your immediate manager.

2. Email Policy

Email has now become a vital business tool for communicating internally and with clients and suppliers. However, because of its flexibility and general availability, the use of email carries with it several significant risks and all users must remain vigilant and adopt good practice when sending and receiving emails.

2.1. Sending and Receiving Email

The organisation provided email address must always be used when communicating with others on official business. You should not use a personal email address for this purpose. Guidelines on the sending of classified information (information classified as Internal, Restricted or Confidential) via email must be observed at all times. These are set out in the document, DL_ISMS A 0802 Information classification policy.

All emails sent from an organisational email address remain the property of Digicore Ltd and are part of the corporate record. All organisation emails should be considered to be official communications from the organisation and treated accordingly.

The organisation maintains its legal right to monitor and audit the use of email by authorised users to assess compliance to this policy. This will be done in accordance with the provisions of relevant legislation.

Deletion of an email from an individual account does not necessarily mean that it has been permanently removed from the organisation's IT systems and such emails may still be subject to audit and review.

All e-mails sent from the organisation to recipients outside of the organisation will carry the following disclaimer:

> *"The information contained in this message is intended for the addressee only and may contain classified information. If you are not the addressee, please delete this message and notify the sender; you should not copy or distribute this message or disclose its contents to anyone. Any views or opinions expressed in this message are those of the individual(s) and not necessarily of the organisation. No reliance may be placed on this message without written confirmation from an authorised representative of its contents. No guarantee is implied that this message or any attachment is virus free or has not been intercepted and amended."*

Users should remain aware that it cannot be guaranteed that an email will be received or read by a recipient and that messages can be interpreted in different ways according to the culture, role and even prevailing mood of the individual reading it. You should therefore always consider whether the use of email is an appropriate means of conveying the information involved and whether an alternative such as the telephone would be preferable, particularly if the message is urgent or complex.

Considerable care must be taken when addressing emails that include classified information to prevent accidental transmission to unauthorised recipients. Users should also avoid sending unnecessary messages to distribution lists..

Emails from an organisational email address should be considered in the same way as other more formal methods of communication. Nothing should be sent externally which might affect the organisation's reputation or affect its relationships with suppliers, customers or other stakeholders.

Users should not send emails containing material which is defamatory, obscene, or which a recipient might otherwise reasonably consider inappropriate.

Official organisation email addresses and facilities should not be used:

- for the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, internally or to other organisations
- to send material that infringes the copyright or intellectual property rights of another person or organisation
- for activities that corrupt or destroy other users' data or otherwise disrupt the work of other users
- to distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- to send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others
- to convey abusive, threatening or bullying messages to others
- to transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs
- for the transmission of defamatory material or false claims of a deceptive nature
- for activities that violate the privacy of other users
- to send anonymous messages - i.e., without clear identification of the sender
- for any other activities which bring, or may bring, the organisation into disrepute

2.2. Maintaining your email account

Your mailbox will be set up with a limitation on its size. You should manage your email account(s) to remain within the mailbox size limit, making use of the archiving facility included in most email clients where possible. If your mailbox is full, kindly contact the IT Security Unit for advice.

Computer viruses, adware and other malware are small programs that can have a negative effect on your computer and your use of the internet and can expose the organisation's information to extreme risk. Such viruses can be inadvertently downloaded and installed via emails. The organisation provides anti-virus software which runs on every computer and should detect any viruses.

If you believe you may have a virus or you have been sent an email that may contain one, please report this to the IT Security Unit immediately. Do not open any attachments you believe may contain a virus.

In addition, you must not:

- transmit by email any file attachments which you know to be infected with a virus
- download data or programs of any nature from unknown sources
- disable or reconfigure the installed anti-virus system operating on a computer used to access email facilities

- forward virus warnings other than to the IT Security Unit

If a computer virus is deliberately or accidentally sent to another organisation, Digicore Ltd could be held liable if the transmission could be considered negligent.

2.3. Email Monitoring

Email usage within the organisation system is monitored and recorded centrally in order to:

- plan and manage its resource capacity effectively
- assess compliance with policies and procedures
- ensure that standards are maintained
- prevent and detect crime
- investigate unauthorised use

If a manager suspects that the email facilities are being abused by a user, they should contact the IT Security Unit. All such reports will be investigated according to documented procedures and where appropriate, evidence provided. There is also a requirement to provide such information to regulatory or legislative bodies in accordance with the law.

Users must not access another user's email account unless they have obtained permission from the owner of the account or their line manager. In such cases this should be for legitimate business reasons and only emails which may reasonably be judged to be relevant to the question in hand should be opened.

3. Access Control

The control of access to our information assets is a fundamental part of a defence in depth strategy to information security. If we are to effectively protect the confidentiality, integrity and availability of classified data then we must ensure that comprehensive controls are in place.

Access control requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation that may apply
- The regulatory framework in which the organisation and the system operates
- Contractual obligations to third parties
- The threats, vulnerabilities and risks involved
- The organisation's appetite for risk

Business requirements should be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

In addition to the specific requirements, several general principles will be used when designing access controls for Digicore's systems and services. These are:

- **Defence in Depth –** security should not depend upon any single control but be the sum of several complementary controls
- **Least Privilege –** the default approach taken should be to assume that access is not required, rather than to assume that it is
- **Need to Know –** access is only granted to the information required to perform a role, and no more
- **Need to Use –** Users will only be able to access physical and logical facilities required for their role

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

3.1. User Authentication for External Connections

Where remote access to the network is required via VPN, a request must be made via the IT Security Unit. A policy of using two factor authentication for remote access should be used in line with the principle of "something you have and something you know" to reduce the risk of unauthorised access from the Internet.

3.2. Supplier Remote Access to the Organisation Network

Partner agencies or 3rd party suppliers must not be given details of how to access the organisation's network without permission from the IT Security Unit. Any changes to supplier's connections (e.g. on termination of a contract) must be immediately sent to the IT Security Unit so that access can be updated or ceased. All permissions and access methods must be controlled by the IT Security Unit.

3.3. User Authentication and Password

A strong password is an essential barrier against unauthorised access. Unfortunately, this area is often proven to be the weak link in an organisation's security strategy and a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometric techniques.

- User passwords are changed at least every 90 days.
- Passwords must be at least Twelve(12) characters in length and consist of numeric, special character , upper case and lower case alphabetic characters.
- Users cannot submit a new password that is the same as any of the last five passwords he / she has used.
- Users should change passwords if there is any suspicion the password could be compromised.
- Passwords cannot contain the username.

3.4. User Responsibilities

To exercise due care and ensure the security of its information, Digicore Ltd expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day-to-day roles..

4 Mobile Computing

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows. However, as the capabilities increase so do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of an office building.

Mobile devices include items such as:

- Macbooks
- Laptops
- Tablet devices
- Smartphones

4.1. Physical Protection

- You must ensure that the device is transported in a protective case when possible and is not exposed to situations in which it may become damaged.
- Do not leave the device unattended in public view, such as in the back of a car or in a meeting room or hotel lobby.
- Do not remove any identifying marks on the device such as a company asset tag or serial number.
- Ensure that the device is locked away when being stored and that the key is not easily accessible.
- Faults with the device must be logged with the IT Security Unit.
- Do not add peripheral hardware to the device without the approval of the IT Security Unit.
- The IT Security Unit should be consulted before the device is taken out of the country.

4.2. Overlooking

- When in public places, ensure that you position the device such that unauthorised people cannot view (or take photographs or video of) the screen

5. Bring Your Own Device (BYOD)

The purpose of this policy is to set out the controls that must be in place when using mobile devices that are not owned or provided by the organisation. It is intended to mitigate the following general risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of classified information through observation by the public
- Introduction of viruses and malware to the network
- Loss of reputation

It is important that the controls set out in this policy are observed at all times in the use and transport of BYOD mobile devices. It is a joint decision between the organisation and the owner of the device concerning whether any device will be used for business purposes.

Such use is not compulsory and the employee has the right to decide whether the additional controls placed on the device by the organisation are acceptable and therefore whether they choose to use the device for business purposes.

5.1. BYOD Assessment Process

Individuals must not use their own devices to hold and process company information unless they have submitted a request to do so, and that request has been formally approved. It is Digicore Ltd's policy to assess each BYOD request on an individual basis to establish:

- the identity of the person making the request
- the business reason for the request
- the data that will be held or processed on the device
- the specific device that will be used

Requests should be submitted to the IT Security Unit.

The general principle of this policy is that the degree of control exercised by the organisation over the BYOD device will be appropriate to the sensitivity of the data held on it. The information classification scheme in use within Digicore Ltd is described in the document - DL_ISMS A 0802 Information classification policy

5.2. Audit and monitoring

To ensure its data is adequately protected, it is important for Digicore Ltd to be able to monitor and audit the level of compliance with this policy. The level of monitoring and audit will be appropriate to the classification of the information held on the device.

The methods and timing of monitoring and audit should be such that the device owner's privacy is not invaded and should be in line with applicable privacy legislation. In general, monitoring of usage outside of business hours should be avoided.

In the event of the device being lost or stolen, the owner must inform the IT Security Unit as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it. Digicore Ltd reserves the right to remote wipe the device where possible as a security precaution. This may involve the deletion of non-business data belonging to the device owner.

Upon leaving the organisation, the device owner must allow the device to be audited and all business-related data and applications removed.

6. Software

Digicore Ltd uses many types of computer software to perform its business operations and relies upon the correct functioning and security of that software at all times. It is imperative therefore that steps are taken to ensure that only approved software is used within the organisation and that no classified information is put at risk.

This policy sets out how software will be acquired, registered, installed and developed within Digicore Ltd.

7. Network Security

The use of networks is an essential part of the day-to-day business of Digicore Ltd. Networks not only connect many of the components of business processes together, but they also link the organisation with its suppliers, customers, stakeholders and the outside world.

The fact that so much information runs through our networks makes them a target for those who would try to steal that information and disrupt our business. Therefore, these networks need to be protected to ensure that the confidentiality, integrity and availability of our vital information is always assured.

The effective protection of our networks requires that we adopt good practices in information security covering the design, implementation, operation and management of the networks and that we ensure that everyone involved follows these practices.

This policy sets out Digicore Ltd's rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure.

7.1. Network Security Design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on a specific set of requirements that are established early in the process. This policy does not attempt to specify how individual networks should be designed and built but provides guidance for the standard building blocks that should be used.

A network design should be based on a clear definition of requirements which should include the following security-related factors:

- The classification of the information to be carried across the network and accessed through it
- A risk assessment of the potential threats to the network, considering any inherent vulnerabilities
- The level of trust between the different components or organisations that will be connected
- The hours of availability and degree of resilience required from the network
- The geographical spread of the network

- The security controls in place at locations from which the network will be accessed
- Security capabilities of existing computers or devices that will used for access

7.2. Defence in Depth

A “Defence in Depth” approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network.

7.3. Network Segregation

The principle should be adopted that a network should consist of a set of smaller networks segregated from each other based on redundancy or security considerations.

7.4. Perimeter Security

At all perimeter/s between the AWS cloud network and an external network (such as the Internet) effective measures should be put in place to ensure that only authorised network traffic is permitted. This will usually consist of Network Access Control Lists.

Servers that are intended to be accessed from an external, insecure network (such as web servers) should be located in a Public Subnet.

7.5. Public Networks

Where information is to be transferred over a public network such as the Internet, strong encryption via SSL must be used to ensure the confidentiality of the data transmitted.

7.6. Wireless Networks

Wireless networks should be secured using WPA2 encryption. WEP and WPA should not be used.

7.7. Remote Access

Where there is a requirement for remote access to the organisation’s network the following controls will be used:

- A Virtual Private Network (VPN) will be used providing session encryption using SSL
- Two factor authentication

Remote access should be granted on an “as required” basis rather than for all users by default.

7.8. Network Intrusion Detection

For networks with high security requirements an Intrusion Prevention System (IPS) should be considered, although its implementation should be approached with caution to avoid a high degree of false positives with corresponding disruption to service to users.

7.9. Network Security Management

Once networks have been designed and implemented based on a clear set of security requirements, there is an ongoing responsibility to manage and control the secure

networking environment to protect the organisation's information in systems and applications.

7.10. Logging and Monitoring

Logging levels on network devices should be configured in accordance with organisation policy and logs monitored on a regular basis.

7.11. Network Changes

All changes to network Appliances will be subject to the change management process and appropriate risk assessment, planning and back-out methods put in place. The Change Management Portal should be updated whenever such changes are carried out so that a current and accurate picture of the network is always maintained.

7.12. Network Security Incidents

Events which are deemed to be network security incidents should be recorded and managed according to the incident management process. Major network outages should be managed via the Major Incident Management Process which provides for the invocation of aspects of the business continuity plan where appropriate.

8. Backups and Storage Media Handling

8.1. Backups

Regular backup of essential business information must be taken to ensure that the organisation can recover from disaster, media failure or error. An appropriate backup cycle must be used and fully documented. Any 3rd parties that store organisation information must also be required to ensure that the information is backed up.

Full documentation of the recovery procedure must be created and stored.

Regular restores of information from backup media must be performed to ensure the reliability of the back-up media and restore process.

8.2 . Storage Media

Removable computer media (e.g. tapes, disks, cassettes and printed reports) must be protected to prevent damage, theft or unauthorised access.

Storage media being stored or transported must be protected from unauthorised access, misuse or corruption.

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by the Product and Engineering Units.

Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

Storage media that is no longer required must be disposed of safely and securely to avoid data leakage.

9. Cryptographic Policy

A key component in the set of controls available to organisations to protect their classified information is the use of cryptographic techniques to “scramble” data so that it cannot be accessed without knowledge of a key.

Cryptographic controls can be used to achieve a number of information security-related objectives, including:

- **Confidentiality –** ensuring that information cannot be read by unauthorised persons
- **Integrity –** proving that data has not been altered in transit or whilst stored
- **Authentication –** proving the identity of an entity requesting access to resources
- **Non-repudiation –** proving that an event did or did not occur or that a message was sent by an individual

The need for cryptographic controls will be highlighted from the Digicore Ltd risk assessment and will obviously not be applicable in all cases. However where their use can provide the required level of protection they should be applied.