I.T SECURITY POLICY

Key Information

Prepared by:	DCA & DCS
Current version:	V2
Last reviewed:	November 2018
Next review date:	June 2021
Person responsible for review:	Compliance Officer
Approver	CEO

Document History

Version	Summary of Amendments	Author	Date	Pages
1	New document	DCA & DCS	November 2018	10
2	Reviewed	DCA & DCS	15 June 2020	9

1. Overview

This Policy sets out appropriate rules and guidelines to protect information and information technology services, systems, and equipment of Duxton Capital (Australia) Pty Ltd (DCA), Duxton Capital Services Pty Ltd (DCS) and associated IT infrastructure.

2. Scope of Policy

This Policy applies to all DCA & DCS employees, consultants, and any other parties (e.g. business partners, service providers, suppliers etc.) with respect to information assets and systems.

3. Review and Evaluation

This Policy will be reviewed annually. Any changes to the Policy will need to be approved by senior management of DCA & DCS.

4. Policy Principles

4.1 Acceptable and Unacceptable Use of DCA & DCS IT

DCA & DCS IT must be used in a lawful, ethical and responsible manner, and in accordance with other applicable DCA & DCS policies, and any additional terms of use that may apply to software or services DCA & DCS IT is provided for use in business activities of DCA & DCS. Some non-business personal use may be allowed but is considered a privilege and not a right and should not interfere with work the user is required to perform. If that privilege is abused, it will be treated as a breach of this policy

- Users must take required steps to ensure data under their possession is protected and their account is protected from unauthorised use
- Use of DCA & DCS IT or personal devices must not put at risk the IT environment, nor operations, assets, data integrity or reputation of the business
- Users must not add, remove, or modify any software or install malicious software on DCA & DCS IT
- Users are expected to report actual or suspected breaches of this Policy or other security incidents immediately that may pose a threat to the security of DCA & DCS IT

4.2 Information Security

Information security ensures that both physical and digital data is protected from unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction.

The following security controls represent the areas of baseline control requirement for DCA & DCS:

- Confidentiality – information is not made available or disclosed to unauthorised individuals, entities, or processes
- Information Integrity – Protection against unauthorised modification of critical information
- Availability – Assurance that critical resources are accessible to authorised entities upon demand

Security control mechanisms must be applied in each category in accordance with application and classification of data. It is the responsibility of all employees of DCA & DCS to ensure that the necessary level of protection is applied.

4.3 Contract / Third-Party Access

Third-party vendor and service providers should only be authorised on a confidential basis to access DCA & DCS IT for business purposes and in accordance with the principle of Least Privilege, which requires that an individual, program or system process not be granted any more access privileges than are necessary to perform the task.

4.4 Infrastructure Security

All infrastructure systems including servers, desktops, laptops, and network equipment installed within DCA & DCS must comply and be configured according to appropriate architectures and standards set by DCA IT.

4.5 Network Control

The role of network security is to protect DCA & DCS IT infrastructure from all types of cyber threats including viruses, worms and trojans; zero-day attacks; hacker attacks; denial of service attacks; spyware and adware.

4.6 Logical Control

Roles, privilege, and profiles assigned to users is in accordance with Least Privilege.

Remote access requires authorisation from the CEO for use of the VPN or RDS platform.

4.7 Disaster Recovery

DCA & DCS has a DRP that will help to recover services within an acceptable time frame. DRP should be tested on an annual basis and updated both annually and whenever there is significant change to DCA IT.

4.8 Physical Security

4.8.1 Asset Security

- Employees issued with portable equipment must agree to personal responsibility for the equipment
- Portable equipment must be secured when not in use e.g. locked and stored appropriately
- Disposal of DCA & DCS IT assets (e.g. computers, laptops, printers, hard drives etc.) must be coordinated via the Office Manager to ensure that all data is removed using approved data removal tools and procedures
- All software must be removed from devices prior to disposal to prevent potential breaches of software licence
- The network server is to be secured in a locked rack in the server room

4.8.2 Building Security

- Doors must be locked and alarmed when the office buildings are unattended or after hours. Offices are monitored by a 24-hour alarm monitoring service
- Access must be changed / disabled when a user leaves DCA & DCS (e.g. alarm code/fob access)

- Users must immediately report loss or theft of keys and/or access hardware to the Office Manager or HR Manager

4.9 Cyber Security

Cyber security is put in place to protect DCA & DCS IT digital data from unauthorised access, attack, or damage by implementing various processes, technologies, and practices. The following approach should be adopted for keeping DCA & DCS IT digital data safe and secure or when reviewing requests for business or personal data.

4.9.1 Social Engineering

Through the process of social engineering, attackers manipulate people into giving them access to sensitive information. The most common social engineering attacks include:

Ransomware: Victims are tricked into installing or downloading malware via credible looking emails. Money is demanded by the criminals to restore access

Phishing: Tactics include deceptive emails, websites, and text messages to steal information

Spear Phishing: Email is used to carry out targeted attacks against individuals or businesses

Pretexting: Uses false identity to trick victims into giving up information

Baiting: An online and physical social engineering attack that promises the victim a reward

Scareware: Victims are tricked into believing that malware or illegally downloaded content is installed on their machines and that if they pay, it will be removed

Quid Pro Quo: Relies on an exchange of information or service to convince the victim to act

Tailgating: Relies on human trust to give the criminal physical access to a secure building or area

Vishing: Urgent voicemails convince victims they need to act quickly to protect themselves from arrest or other risk

Water Holing: An advanced social engineering attack that infects both a website and its visitors with malware

4.9.2 Password Protection

Use strong passwords or passphrases that are hard to guess to protect your devices or accounts that hold important business information. When it comes to creating passwords, the longer they are, the stronger they are. Passphrases are a series of words that are longer and easier to remember and harder to guess than traditional passwords.

Frequently change your passwords every few months and do not share passwords. If you use the same password for everything, once someone has your password, all your accounts are potentially under attack.

Do not include the following things in your passwords/passphrases:

- Repeated characters

- Single dictionary words, your street address, or numeric sequences (e.g. 1234567)
- Personal information
- Anything that you have used previously

Keep your passwords secure by taking measures to protect them:

- Do not provide your password in response to a phone call or email, regardless of how legitimate it seems
- Do not provide your password to a website you have accessed by following a link in an email, it may be a phishing trap
- If you do not trust a website, do not trust it with your password
- Do not use password protected services on a public computer or over a public wi-fi hotspot
- Treat passwords in the same way you would a PIN and do not use:
  - obvious patterns like 1234, 4321 or 7777
  - postcodes, birthdays or other significant dates and numbers; or
  - write the password down and leave it where it could be accessed.

4.9.3 Password Policy

DCA & DCS has a password policy in place for creating passwords in any business application (excluding email)

- Passwords to be changed at least every 90 days
- Minimum password length of 8 characters
- Passwords cannot be changed more than once a day
- Passwords must be changed if expired
- Passwords cannot be reused within 24 password changes
- Passwords must meet complexity requirements.

Complex password description

- Passwords need to contain characters from three of the following categories:
  - Uppercase letters (A through Z)
  - Lowercase letters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphanumeric characters e.g. ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

- Passwords should not contain the employee's name or user/account name

4.9.4 Email Standards

- Users should use their work email address for business purposes only and not for personal activities
- Users should never use personal email to transmit or conduct business
- Users should not share any personal information in emails
- Users should only open email attachments from trusted and known contacts and businesses
- Suspicious looking emails should be deleted without opening and reported to DCA & DCS IT

4.9.5 Security of Computers and Devices

- Users are responsible for ensuring that their own computers and personal devices containing business information are protected from loss, theft, destruction, and unauthorised disclosure and are always physically secured in an appropriate manner
- Mobile or smart devices that contain business information must be locked with a password or pin code in case of loss or theft
- Users must use a secure internet and Wi-Fi connection for computers and devices outside of the business network as an unsafe internet connection provides a channel into devices that could be exploited for malicious purposes
- Personal computer use at home should not be completed on a corporate machine such as browsing the web, playing games, or undertaking other activities online to protect DCA & DCS IT equipment from the risk of threats
- Contact Office Manager or HR Manager to report lost or stolen equipment immediately

  The DCA & DCS security settings for business laptops is set to the below parameters:

  - Laptop will lock after 15 minutes
  - Laptop will lock after 10 incorrect password attempts

4.9.6 Handling of Sensitive Material

- All employees should adopt a clean-desk policy, meaning that no papers, documents, or files containing private/sensitive data should be left exposed or unattended even for short periods
- Employees should try and minimise the amount of paper printed and produced
- Sensitive information should not be stored in an area where the public or other employees have access or where there is regular traffic of individuals who are unauthorised to view such information

- Sensitive documents should be removed from printers and photocopiers immediately

- Unwanted documents should be disposed of as soon as practically possible using a paper shredder or secure document destruction bin

- Meeting rooms must be cleared of documents on tables or information on whiteboards where employees hold internal or external meetings to ensure no sensitive data is visible to others Limit the use of email to send sensitive material and if sent by email, password protect or encrypt the sensitive material

- Confirm correct email addresses before emails with sensitive information are sent

4.9.7 Handling of Removable Devices

- Avoid using portable storage devices where practically possible

- Removable devices that contain restricted or confidential information should be password protected

- Do not use external hard drives or removable devices from an unfamiliar source

- It is assumed that all removable devices have been scanned for viruses and malware prior to connecting to DCA & DCS IT

4.9.8 Remote Access

- Users to read and acknowledge the DCA & DCS Remote Access User Policy prior to first use

- Users are responsible to ensure remote connection is given the same consideration and security as their on-site connection to the Duxton Network

- Users should only use work email accounts and approved file sharing applications for work-related matters.

- Remote access platforms (VPN/RDS) must only be used on approved DCA & DCS corporate devices

- Account logins and passwords to corporate devices should not be shared with anyone, including family members

4.9.9 Social Media and the Internet Access Standards

Accessing the Internet through corporate IT infrastructure should be used for business-related purposes. The internet may be accessed for incidental use provided that personal use is moderate in time, does not incur significant cost to DCA & DCS and does not interfere with the duties of the user or his or her colleagues.

Proper conduct is expected of all users on the Internet, as it is on all public forums and social media sites. Improper conduct includes, but is not limited to:

- Creating or exchanging messages that are offensive, harassing, obscene or threatening

- Defaming DCA & DCS or bringing the company into disrepute

- Personal communications that imply the employer's endorsement of personal opinions

- Visiting web sites containing objectionable (including pornographic) or criminal material Exchanging proprietary information, trade secrets, or any other confidential or sensitive information about the company (unless in the authorised course of their duties)

- Creating, storing, or exchanging information in violation of copyright laws (including the uploading or downloading of commercial software, games, music videos or movies)

- Using Internet enabled activities such as gambling, gaming, conducting a personal business (unless approved in writing) or conducting illegal activities

- Creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email

- Disclosure or sharing of accounts or passwords

4.9.10 Security Incident Management

Any suspected inappropriate or illegal usage of DCA & DCS IT should be reported to the Office Manager or HR Manager immediately. This information will be reported to the CEO for investigation.

All information reported to the Office Manager or HR Manager shall be treated in the strictest confidence. Any reported information will be logged, and relevant action taken, including reporting to relevant management as required.

4.9.11 Data Breaches

Australian law requires the company to take active steps in response to any loss of unauthorised access to private information (e.g. information about investors and our employees). This may include notification of the breach to Federal authorities within 30 days, and there are severe penalties for failure to comply (multimillion dollar). There are similar but stricter laws that apply to foreign data such as the EU GDPR. This is relevant to DCA & DCS due to interactions with European clients.

Personal information includes any information or an opinion about an identified individual. A person's name, signature, home address, email address, telephone number, date of birth, bank account details and employment details will generally be personal information.

A breach of data can include:

- Loss of an IT device e.g. USB, smart phone, tablet, or computer

- Unauthorised internal access to personal information

- Accidental release of client information (e.g. wrong email recipient)

- A contractor being hacked or losing DCA & DCS data

To reduce the risk of a breach:

- Do not use factory default passwords or those that are easy to guess (i.e. password1)

- Maintain control of administration privileges of company systems

- Control information access based on Least Privilege

If a breach is suspected or has occurred immediately notify the HR Manager, Office Manager or Head of Legal, Governance & Reporting.

4.10 Breaches of This Policy

Breaches of this Policy may result in suspension of access to DCA & DCS IT and/or disciplinary procedures. Breaches of the Policy may also be reported to external parties as required under law.

5. Definitions

In this document:

Account Holder means a person who has been provided with a password protected account to access DCA & DCS IT.

DCA & DCS means Duxton Capital (Australia) Pty Ltd & Duxton Capital Services Pty Ltd

DCA & DCS **IT** means any computing or communications device or infrastructure; computer or communications program or software; service that provides access to the internet or information in electronic format; computer network, website or online forum, including social media; electronic data stored or processed in any of the above, that is owned, managed, hosted or provided by DCA & DCS or a third-party provider on DCA & DCS's behalf.

DRP means Disaster Recovery Plan.

Employee means an individual who works casually, part-time, or full-time for Duxton Capital (Australia) Pty Ltd & Duxton Capital Services Pty Ltd under a contract of employment.

EU GDPR means European Union General Data Protection Regulation.

Least Privilege is where an individual, program or system process is not granted any more access privileges than are necessary to perform the task.

RDS refers to Remote Desktop Services that allows a user to take control of a remote computer or virtual machine over a network connection.

Senior Management means Group Chairman or CEO.

USB means a small external flash drive that can be used with any computer that has a USB port.

User means any person who accesses DCA & DCS IT.

VPN is a virtual private network.