Newcastle
Level 2, 117 Scott Street,
Newcastle NSW, 2300
PO BOX 283, Newcastle, NSW, 2300
P: +61 2 4929 6377
F: +61 2 4929 1556

Melbourne
Suite 1.2, 415 Riversdale Road,
Hawthorn East, VIC, 3123
P: +61 3 9001 0300
F: +61 3 9001 0311

Sydney
Level 34, 50 Bridge Street,
Sydney, NSW, 2000
P: +61 2 4921 2450
F: +61 2 4929 1556

www.nsxa.com.au

Incorporating
NSX Limited
ABN: 33 089 447 058
National Stock Exchange of Australia Limited
ABN: 11 000 902 063
SIM Venture Securities Exchange Limited
ABN: 41 087 708 898

Information Technology Policy

This policy documents the Computer Use Policy within the NSX Group

Table of Contents

Table of Figures

1 General Computing Policies

1.1 Introduction

All NSX's IT facilities and information resources remain the property of NSX and not of particular individuals, teams or departments (Note1). By following this policy we'll help ensure IT facilities are used:

- legally;
- securely;
- without undermining NSX;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so they remain available.

The policy relates to all Information Technology facilities and services within the NSX Group provided by NSX. All Directors, Employees and contractors are expected to adhere to it.

1.2 Relevant Legislation

Relevant legislation is produced as Appendix A at the end of this document for the reference of employees.

2 Policies

2.1 Access to Computing Equipment

The majority of employees will have access to a PC or related equipment. This has been supplied to assist in making your job more efficient and more enjoyable. The company has networked all computer facilities and linked the system to both email and Internet access.

Sensitive data centre rooms are locked and can only be entered by authorised personnel.

The following statements should also be used as a guide for access and use of the commuting environment:

- Don't attempt to gain unauthorised access to information or facilities. If you don't have access to information resources you feel you need, contact your IT Support person.
- Don't disclose personal system passwords or other security details
- to other Employees, contractors or external agents and don't use anyone else's username; this compromises the security of NSX. If someone else gets to know your password, ensure you change it or get IT Support to help you.
- If you leave your PC unattended without logging off, you are responsible for any misuse of it while you're away.
- ALWAYS check storage media for viruses, even if you think they are clean (contact IT Support to find out how). Computer viruses are capable of destroying NSX's information resources. It is better to be safe than sorry.

2.2 Username and Password Security

Usernames and password issued to employees should be kept confidential and changed regularly. Crucial systems such as access to banking facilities and the NSX trading engine have password regimes imposed on to them.

Usernames and passwords should not be disclosed to other especially those external to the company without authorisation.

Disclosure to other Employees, contractors or external agents may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with the IT Support. If the password is disclosed for a one-off task, the owner must ensure that his / her password is changed (by contacting IT Support) as soon as the task is completed.

2.3 Abide by software licencing requirements

Employees are to take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

2.4 Personal Use of Computers Policy

Access to these facilities is for business purposes only and not for private use. IT Support monitors traffic to and from the server, as well as the overall network. Where access to the Internet is required as part of your job, you will be given appropriate password access and we expect you to treat this password as confidential.

Limited personal use of computers is only allowed during your lunch break if you are taking your lunch at your desk.

Playing of computer games is prohibited.

Sending and receiving personal email, and browsing the Internet is permitted so long as such use does not:

- incur specific expenditure for NSX;
- impact on your performance of your job (this is a matter between each member of employees and their line manager);
- break the law; or
- bring NSX into disrepute.

2.5 Electronic monitoring

Any information available within IT facilities must not be used to monitor the activity of individual employees in anyway (e.g. to monitor their working activity, working time, files accessed, Internet sites accessed, reading of their email or private files etc.) without their prior knowledge.

Exceptions are:

- in the case of a specific allegation of misconduct, when the Management Team can authorise accessing of such information when investigating the allegation;
- when the IT Support section cannot avoid accessing such information whilst fixing a problem. In such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary. In the former case their access to IT facilities may be disabled pending investigation.

2.6 Electronic Media Policy

The use of privately sourced Floppy Disks, CD-ROMS, DVDs, USB Drives, Smartphones and other devices and media on company equipment can be sources of viruses and other malicious software. All media used for transferring data should be company supplied and virus checked before use.

2.7 Viruses, Trojans and Other Malicious Software Prohibition

Even though NSX has taken all reasonable care to ensure safety and a virus-free computer environment, we are all aware of the problems a virus can cause. Employees should take care to not go

to websites that could potentially introduce a virus into the NSX network or open emails from unknown sources.

Employees are to report immediately to IT Support any suspicious websites or emails that they have visited or opened or if they believe their computer has become infected with a virus.

2.8 Offensive Material Prohibition

Use of computers to distribute inappropriate and offending material can be cause for disciplinary action. Such material can be but is not limited to pornographic, hate or flame mail and racist material.

Employees are prohibited from down loading such material and should report any occurrence to IT Support and their line manager.

You are a representative of NSX when you're on the Internet using email and NSX equipment. You should observe the following behaviours:

- Make sure your actions are in the interest (and spirit) of NSX and don't leave NSX open to legal action (e.g. libel).
- Avoid trading insults with other people using the Internet with whom you disagree.
- Obscenities/Pornography: Don't write it, publish it, look for it, bookmark it, access it or download it.

2.9 Bring your own devices (BYOD) policy

2.9.1 Devices

Device may be smartphones, tablets, netbooks, computers and other electronic devices as approved by NSX.

The use of a smartphone in connection with NSX's business is a privilege granted to employees through approval of their management. NSX reserves the right to revoke these privileges in the event that users do not abide by the policies and procedures set out below.

The following policies are aimed to protect the integrity of NSX data and ensure it remains safe and secure under NSX control. Please note that there may be limited exceptions to these policies owing to device limitations between vendors.

References to the word "device" below includes, but is not limited to, Android, BlackBerry, iPhone, iPad, tablet, Windows mobile or other smartphones and devices.

Users of Personal Smartphones must agree to all terms and conditions in this policy to be allowed access to those NSX services.

2.9.2 Device security

Irrespective of security precautions mentioned here, you are expected to use your device in an ethical manner and in accordance with this policy.

- Your device must lock itself with a PIN (personal identification number set by you).
- If left idle, your device must automatically activate its PIN after a maximum time-out period of 5 minutes. In the event of loss or theft of your device, you must inform NSX within 3 working days. Your device will lock your account after 5 failed login attempts. Your device or application will lock every 5 minutes, requiring re-entry of your password
- The password must contain at least one letter or number (except on devices that cannot accept alphanumeric passwords)
- Your device may be remotely wiped if: (i) you lose the device; (ii) you terminate employment with NSX; (iii) the IT section detects a data or policy breach or virus; or (iv) if you incorrectly type your password 10 consecutive times.

This means your personal data is still vulnerable, and thus it is recommended you also set a device password and take additional security precautions.

2.9.3 Tampering

Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' or 'rooting' your smartphone.

2.9.4 Liability

A personal smartphone can be connected to the NSX infrastructure or services, but the user is personally liable for their device and carrier service costs. Users of personal smartphones are not eligible (except by prior agreement) for reimbursement of expenses for hardware or carrier services.

2.9.5 Access

Employees that purchase a device on their own that is not in line with our standard approved device may not be able to or allowed to have their devices added to our servers. [It is highly recommended that the employee refer to NSX IT support to review approved devices. Users of personal smartphones are not permitted to connect to NSX infrastructure without documented consent from NSX IT support. Furthermore, NSX reserves the right to disable or disconnect some or all services without prior notification.

2.9.6 Disclaimer

NSX hereby acknowledge that the use of a personal smartphone in connection with NSX business carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the operating system, errors, bugs, viruses, downloaded malware, and/or other software or hardware failures, or programming errors which could render a device inoperable.

2.10 Spam, Junk email, Pornography Prohibition

Receipt of offending material by an employee member should be immediately deleted.

2.11 Email Policy

2.11.1 When to use email

- Use it in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. Think about and check messages before sending (just as you would a letter or paper memo).
- Use the phone (including voicemail if no reply) for urgent messages (email is a good backup in such instances).
- Use NSX's shared drives (not email) to communicate all relatively static information (e.g. policy, procedures, briefing documents, reference material and other standing information). Record information on the shared drives in a well structured manner. Use email merely as a pointer to draw attention to new and changed information on the shared drives.

2.11.2 Use of Distribution Lists

- Only send Email to those it is meant for; don't broadcast (i.e. send to large groups of people using email distribution groups) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer performance and wastes disc space.
- Use the standard distribution lists for work related communication only.
- Don't broadcast emails with attachments to large groups of people either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

2.11.3 General points on email use:

- When publishing or transmitting information externally be aware that you are representing NSX and could be seen as speaking on NSX's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.
- Check your in-tray at regular intervals during the working day.
- Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary or as required by NSX audit, compliance and surveillance activities.
- Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions / decisions of a colleague).
- Don't forward emails warning about viruses (they are invariably hoaxes and IT Support will probably already be aware of genuine viruses - if in doubt, contact them for advice).

2.11.4 Email etiquette

- Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are also copying another group of people.
- Make your subject headers clear and relevant to your reader(s) eg Don't use subject headers like "stuff" Don't send a subject header of, say "accounts" to the accountant
- Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.

2.11.5 Use of third party email addresses

- Employees will commonly have one or multiple third party email addresses originating from Hotmail or google gmail. Third party email address are **not** to be used for work purposes (that is creation of emails, forward or replies etc) as these email addresses, if used would, confuse the intending recipient.
- Work email's are not to be stored on private third party emails which would override NSX's archiving of such data

2.12 Installation of Software and Software Upgrades

Employees should obtain permission from IT Support before installation of any software on equipment owned and/or operated by NSX.

Upgrades of software should also be performed with the advice of IT Support. In most cases IT Support will have confirmed NSX equipment to require an administrator username and password to perform installation of software.

2.13 Data security, storage and privacy

- Keep master copies of important data on NSX's network and not solely on your PC's local drive or other storage media. Otherwise it will not be backed up and is therefore at risk.
- Ask for advice from IT Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill.
- Be considerate about storing personal (non- NSX) files on NSX's network.
- Don't copy files which are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disc space unnecessarily and can circumvent the master/salve relationship of documents. Local storage of documents overrides NSX's archiving procedures.

2.14 Care of Equipment

- Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting IT Support.
- Don't take food or drink into rooms which contain specialist equipment like servers. Access to such rooms is limited to authorised employee.

2.15 Intellectual property rights and ownership of software

In-house software is written by employees using NSX's equipment. It is NSX's property and must not be used for any external purpose.

3 Disaster Recover Policy

3.1 Requirement for policy with respect to computing equipment and personnel

NSX maintains disaster recovery procedures and employees must abide y these procedures I the event of a disaster.

3.2 Reference to Disaster Recover Procedures

For further information Employees should reference the NSX Disaster Recover Procedures.

4 Physical Access to Data Server Room

The data center and associated rooms must only be accessible by approved persons

The doors to the data center are to remain locked when no one is physically present with in the room or not performing required work associated with the servers.

5 Privacy of Information

If you're recording or obtaining information about individuals make sure you are not breaking the relevant legislation (your IT Manager or Line Manager can give you more information).

This information also covers publicly available email addresses used in newsletters. Use of these email addresses should be with the permission of the owner of the email address.

Employees should abide by the Relevant Privacy legislation and policies of NSX.

6 Domain Name registration

All domain names for projects/activities must be registered through the General Manager & company Secretary so that NSX assets can be recorded and accounted for. The NSX Board should also be informed before domain names and websites are activated for use.

This requirement must be observed in all instances. Users should note it is the NSX who owns and controls the site not the person who registers the name.

7 Commercial Use

IT Resources must not be used for private commercial purposes.

8 NSX's Liability

The NSX accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from personal use of the NSX's IT Resources.
- Loss of data or interference with personal files arising from the NSX's efforts to maintain the IT Resources.

9 Confidential Information

Authorised Users have a duty to keep confidential:

- All NSX data; and
- Information provided in confidence to the NSX by other entities.

Each staff member is under a duty not to disclose NSX business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose an Employee to disciplinary action.

10 Obtaining approvals under the policy

Application to the General Manager and IT support whenever an employee wishes to have approval under this policy. For example connecting their own electronic device to the NSX infrastructure.

11 Reporting of breaches of this policy

11.1 Self Reporting

If an Employee becomes aware that they may have breached a policy they should report it to IT Support or their line manager as soon as possible. If practicable they should also attempt to correct the breach and if necessary with the help of IT Support.

11.2 Reporting other employees

If employees become aware of a significant contravention of this policy they should report it to the General Manager. When in doubt they should discuss the possible breach with their line manager, IT support, or the General Manager.

12 Disciplinary Measures

Deliberate and serious breaches of the policy will lead to disciplinary measures which may include the offender being denied access to computing facilities, disciplinary action or termination of employment.

13 APPENDIX A – Australian Federal Law

13.1 Federal Law governing Computer Security

CRIMES ACT 1914

SECTION 76A

(1)In this Part, unless the contrary intention appears:

"carrier" means:
(a) a general carrier within the meaning of the Telecommunications Act 1991; or
(b) a mobile carrier within the meaning of that Act; or
(c) a person who supplies eligible services within the meaning of that Act under a class licence issued under section 209 of that Act;
"Commonwealth" includes a public authority under the Commonwealth;
" Commonwealth computer" means a computer, a computer system or a part of a computer system, owned, leased or operated by the Commonwealth;
"data" includes information, a computer program or part of a computer program.

(2)In this Part:
(a) a reference to data stored in a computer includes a reference to data entered or copied into a computer; and
(b) a reference to data stored on behalf of the Commonwealth in the computer includes a reference to:

(i) data stored in the computer at the direction or request of the Commonwealth; and
(ii) data supplied by the Commonwealth that is stored in the computer under, or in the course of performing, a contract with the Commonwealth.

SECTION 76B

(1) A person who intentionally and without authority obtains access to:
(a) data stored in a Commonwealth computer; or
(b) data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
is guilty of an offence.
Penalty: Imprisonment for 6 months

(2)A person who:
(a) with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
(b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defence or international relations of Australia;
(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;
(iii) the enforcement of a law of the Commonwealth or of a State or Territory;
(iv) the protection of public safety;
(v) the personal affairs of any person;
(vi) trade Secrets;
(vii) records of a financial institution; or
(viii) commercial Information the disclosure of which could cause advantage or disadvantage to any

person.
is guilty of an offence
Penalty: Imprisonment for 2 years

(3)A person who:
(a) has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and
(c) continues to examine that data;
is guilty of an offence.
Penalty for a contravention of this subsection: Imprisonment for 2 years

SECTION 76C

A person who intentionally and without authority or lawful excuse:
(a) destroys, erases or alters data stored in, or inserts data into a Commonwealth computer;
(b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;
(c) destroys, erases, alters or adds data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
is guilty of an offence.
Penalty: Imprisonment for 10 years

SECTION 76D

(1) A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence.
Penalty: Imprisonment for 6 months

(2)A person who:
(a) by means of a facility operated or provided by the Commonwealth or by a carrier, with intent to defraud any person and without authority obtains access to data stored in a computer; or
(b) by means of such a facility, intentionally and without authority obtains access to data stored in a computer, being data that the person knows or ought reasonably to know relates to:
(i) the security, defence or international relations of Australia;
(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;
(iii) the enforcement of a law of the Commonwealth or of a State or Territory;
(iv) the protection of public safety;
(v) the personal affairs of any person;
(vi) trade Secrets;
(vii) records of a financial institution; or
(viii) commercial Information the disclosure of which could cause advantage or disadvantage to any person.
is guilty of an offence
Penalty: Imprisonment for 2 years

(3)A person who:
(a) by means of a facility operated or provided by the Commonwealth or by a carrier, has intentionally and without authority obtained access to data stored in a computer;
(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and
(c) continues to examine that data;

is guilty of an offence.
Penalty for a contravention of this subsection: Imprisonment for 2 years

SECTION 76E

A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority or lawful excuse:
(a) destroys, erases or alters data stored in, or inserts data into a computer;
(b) interferes with, or interrupts or obstructs the lawful use of, a computer;
(c) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a computer;
is guilty of an offence.
Penalty: Imprisonment for 10 years