IT Acceptable Use Policy (for Staff)

Navitas Pty Ltd
ACN 109 613 309

Document

Document Name	IT Acceptable Use Policy (for Staff)
Responsibility	Chief Technology Officer
Initial Issue Date	10/02/2007

Version Control

Date	Version No.	Summary of Changes	Reviewer Name and Department/Office
10/02/2007	1.0	Initial Release	Navitas IT
27/06/2017	1.1	Extensive review and update of content	Navitas IT
18/02/2018	1.2	Include Shadow IT, BYOD, apply new Policy template format	Navitas IT
09/08/2018	1.3	Add Section 2.15 to cater for people who have access to personal information	Navitas IT
27/02/2019	1.4	Updated Section 2.4 and added Section 2.5	Navitas IT
30/03/2020	2.0	Updated Section 2.17 & changed CIO to CTO	Navitas IT
29/03/2021	3.0	Added Sections 2.8 – IT Assets & 2.11 – Use of Personal Email Address. Updated Section 2.3 to incorporate mandatory MFA requirement. Created Staff only version; Students are in a new & separate document.	Navitas IT

Related Documents

Name	Location
IT Acceptable Usage Policy Individual Acceptance Form	Policy HUB

Contents

1 Purpose and Scope

1.1 Introduction

This IT Acceptable Use Policy ("**Policy**") sets out the global approach of Navitas Limited and its affiliated group companies (together the "**Company**") relating to the minimum requirements that must be met by all users of the IT systems, services and equipment. This Policy supercedes any other IT Acceptable Use Policies published across the Company.

1.2 Purpose

The Company is a professional organisation and all users are expected to use the IT systems, services and equipment in a professional way. This policy represents the minimum requirements that must be met by all users. IT systems, services and equipment is provided only for professional and business purposes.

1.3 Scope

This Policy has been prepared in accordance with the Company's legislative requirements and principles. This Policy is effective across the entire Company and applies only to all **Staff, Contractors and Consultants** ("**users**") of IT systems, services and equipment at any location, including those users using privately owned computers or systems that connect to the Company network resources and applications

2 Policy Statement

2.1 Underlying Principles

All users must adhere to all elements of this policy. The principles of behaviour relating to the use of the Company IT systems, services and equipment include:

- Respect for appropriate legislation and regulations
- Respect for other people and
- Respect of the Company's mission and values

The principles of conduct of users also expect:

- Integrity
- Diligence
- Economy and
- Efficiency
- Common sense

2.2 Role & Responsibilities

All users of the Company IT systems, services and equipment have a responsibility to maintain compliance with this policy and all relevant policies. Additionally, all users have a responsibility to maintain security and to report anything that may be detrimental to the Company.

The Service Desk is responsible for recording all incidents and allocating investigation or remediation work to core services as required. The regional Data Protection Manager is responsible for capturing and escalating data breaches.

2.3 User Accounts & Passwords

You are responsible for any activity that is performed whilst your username is logged on. Do not share your password with any other person (including IT) and do not log in using any other user's credentials.

Passwords are the "key" into the Company's systems - it is your own responsibility to ensure your password is kept secure. There are two key password management practices that make it harder for attackers to access the Company's systems and data.

- Use “Strong Passwords”. These can slow down or often defeat the various attack methods used to compromise IT security. The Company requires you to always use Strong Passwords. A Strong Password is one that is not easily guessed (not your name, family members, pets, relative or anything else that could be attributed to you). Passwords must be minimum of eight characters long and containing a combination of upper and lowercase letters numbers and special characters. Longer passwords (13+ characters) with less complexity (variation in character types) also increase the strength of the password. The stronger the password, the harder it is to guess or crack.
- Always use different passwords for different sites; whilst it’s convenient to re-use the same password for personal logins, ensure the Company’s password is not one that you use elsewhere. Using a unique password for your Company accounts ensures that systems remain secure if any of your personal accounts are compromised and vice versa.

The use of Multi-factor authentication (MFA) is mandatory. To facilitate the implementation users are required to install the appropriate authenticator app on their smartphone. Users without a smartphone will be required to register using SMS notification. When it comes to mobile devices, the use of PIN codes is required if you are using the mobile device to access Company email. Other forms of security such as fingerprint and Iris scanning are also acceptable. If you lose a device that has been used to store process or transmit Company information report this to the service desk, even if it’s your own device.

2.4 Personal Use of Company Computers and IT Facilities

Do not use company email accounts for personal use. Do not store private data on company computers or IT facilities. Occasional use of the company computers and systems is acceptable using the internet e.g. checking bank accounts etc. The same applies to other IT facilities such as Internet connectivity, printing or scanning.

Company IT systems, services and equipment must not be used for the following:

- Gambling or internet gaming
- Any political activity
- Sending offensive, harassing, intimidating or discriminatory messages or attachments, or to transmit offensive, sexually explicit or other inappropriate material
- Downloading malicious software or applications
- Browsing, sharing, downloading from or otherwise accessing illegal websites
- The use of on-line security scanning or hacking/cracking tools[1]
- Share trading (unless you have express permission due to your company role)
- Use of IT systems for personal financial gain, solicitation or private business purposes, e.g. crypto currency mining
- Posting business information on bulletin boards, blogs or forums that are accessible by the public unless you are specifically authorised to do so
- Downloading or storage of data subject to intellectual property or copyright

Specific agreement is required between the Company and the consumer when it provides a service such as Internet for personal use.

2.5 No Outside Internet Use

Company IT systems, services and equipment are only to be used for professional and business purposes. The only exception is the occasional use permitted in 2.4 above. Any form of outside interest use is prohibited, unless the Company has given prior written authorisation. This means that users of the Company’s IT systems, services and equipment must not use, and must not allow any non-Navitas person or organisation to access or use the Company’s IT systems, services and equipment for any purpose.

[1] Unless used as part of a persons documented working duties.

This includes but is not limited to the follow types of actions:

- Sending unsolicited emails to persons
- Using email or social media platforms to solicit interest in goods or services, participation in surveys, events or group activities or links to any third-party URL or hosted sites
- Data mining for personal information including email addresses, telephone numbers, social media profiles or other personal information that may be stored or accessible on the Company's system

2.6 Social Networking Websites

Users must not use Company or student? email as their communications when establishing social network profiles or registering or providing contact details with any third-party service unless given permission to do so. Whilst it is acceptable to associate yourself within your profile as a user, it must be very clear that you are not posting on behalf the Company unless this is a documented part of your job function. Be careful when posting pictures that they do not contain Company information in the background and that you have permission of your co-workers before posting any pictures of them.

The use of social media on the Company IT systems and networks is to be kept to an absolute minimum.

2.7 Equipment, Security & Loss

The Company will supply all the necessary equipment/devices to access its computer systems and networks. Ensure that Company assets are treated with respect. Do not leave any Company assets unattended where they could be stolen or abused. Users are personally responsible for all equipment issued to them by the Company. Lost or stolen devices must be immediately reported to the Company.. Users are responsible for notifying their service providers. All Company assets are to be returned through line management on completion of employment contract.

2.8 IT Asset Management

The following applies in relation to the purchase, tracking, use and disposal of Company provided IT assets:

- **Purchasing:**
  - You must purchase all IT assets through a Company approved purchasing officer and ensure Companyapproved purchasing methods are used, i.e. purchase outright or lease.
- **Tracking:**
  - Relevant information that identifies the IT asset must be retained for the life of the IT asset. This is completed by the IT function.
- **Use:**
  - The IT asset must be used for the period of it's useful life as defined by the Company and then disposed of securely using approved computer recyciling (for purchased or Finance Leased IT assets), or returned to the lessor (for Operating Leased IT Assets).
- **Disposal:**
  - All Company IT assets must be returned before departure from the company to the local IT representative. Any IT asset disposed of must have "One Pass data erasure" applied before being disposed of.

2.9 Shared Printing

Take care when printing sensitive or confidential material to a shared printer. Most printers support the use of password protection and secure print. Contact the Service Desk for further information about this feature if required.

2.10 Information Security Threats

All users are responsible for the security of information that is owned by or entrusted to the Company. All actual or suspect security weakness are required to be immediatelyreported to the Service Desk.

The Company has inbuilt security features and controls in our email system, network and computers that can detect viruses and malware, but it can never protect you and the Company from every threat. Ensure you are familiar with how to recognise fraudulent email (e.g. phishing attacks) or links and websites[2]. Also, be careful with external USB, hard disk and other storage devices where you cannot verify the contents or the source of the device. Users are the first line of defence. Do not click on a link or open a file that you do not recognise.

All users are required to complete assigned Information Security Awareness training in a timely manner.

2.11 Email Forwarding

Automatic or manual forwarding of emails to non-Company email addresses is not permitted. Where there is an approved business requirement exception, it will be considered by the Global Head of Information Security.

2.12 Use of Personal Email Addresses

Personal email addresses are not to be used for work purposes.

2.13 Inappropriate Content

Do not download inappropriate material, store it on your computer or on the Company network, or include within email or other communications means. Inappropriate content includes but is not limited to the following; information or media that could be considered illegal, harassing, offensive, sexually explicit, racist, sexually discriminatory, in violation of other company policies or that could reflect adversely on the Company.

2.14 Software

All software used on the Company provided devices must be approved by Corporate IT. Users may request additional software through their line management where a business justification exists.

2.15 Removable Media

Removable media items including but not limited to USB connected media, Hard Drive, SD or other memory cards or optical media (CD/DVD) are not to be used on Navitas systems or networks without express (documented) permission by Corporate IT.

[2] As advised through security awareness programmes.

2.16 Shadow IT

Shadow IT is a growing concern that needs addressing to ensure the integrity and efficiency of enterprise technology, and to prevent fragmentation of information and processes. Shadow IT is defined as IT systems and solutions outside the ownership or control of Company IT (e.g. Country Office development of a financial monitoring system). The issue is shadow IT remains largely unmanaged and unacknowledged.

Shadow IT is not necessarily detrimental to the Company. However, it can create risks of data loss, corruption or misuse, inefficient and disconnected processes, and fragmented information which must be addressed appropriately.

The following statements apply to all users responsible for the creation and propagation of hardware and software which are not addressed or covered by current IT policies:

- **Ownership:**
  - The Company owns its shadow IT systems and the information and resources remain the property of the organization.
- **Monitoring & Assessment:**
  - Corporate IT is responsible for assessing and monitoring shadow IT systems to determine associated risks, support services, stability, effectiveness, and impact on internal system performance.
- **Accountability & Right to implement:**
  - Irrespective of where they are charged, considering their impact on existing systems and associated risks, proposals of large shadow IT systems (greater than AUD$10,000 or 80 person hours of development) must be presented and approved by the IT Governance group. The Group will ensure that the shadow IT system is aligned to organizational strategic goals and must also be informed of any major changes to such systems as these may affect other IT areas as well.
  - Smaller shadow IT systems (less than AUD$10,000 or 80 person-hours of development) require the approval of the relevant Company Regional Business partner.
- **Security:**
  - One of the most significant areas of concern with Shadow IT relates to security. The potential of external, reputational damage to the organisation from failure or malfunction is greater with shadow IT systems. Providing Corporate IT with details regarding the security and appropriateness of information in such systems is essential. Information Security requirements outlined in the Vendor Assessment Procedure must be followed.

2.17 BYOD

To facilitate remote working the Company allows users the privilege of using their own devices (BYOD). The Company reserves the right to revoke this privilege if users do not abide by the statements below.

- **Acceptable use:**
  - Use of any BYOD device is subject to the same conditions as defined in this policy whilst performing work for the Company using the Companies network to access its services.
- **Devices and Support:**
  - The Company will define and allow a list of devices and operating system versions that it will support for BYOD.
  - Only network connectivity issues are supported by IT; users should contact the device manufacturer or their carrier for operating system or hardware-related issues.
  - Company endorsed Virtual Private Network (VPN) solution is required to be used when connected to the user's home network or authorized third-party network.

- **Reimbursement:**
    - The user is personally liable for all costs associated with his or her device and accessing the company network.
- **Device Security:**
    - The latest version of the operating system (which includes patches) should be maintained at all times.
    - Company endorsed anti-virus software must be installed on the devices at all times.
    - In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
    - Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
    - Users access to Company data is limited based on user profiles defined by IT and automatically enforced.
    - The company will take appropriate action (if possible) on the device if it detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
    - Company data must not be stored on a BYOD device.
- **Risks/Liabilities/Disclaimers:**
    - While Company IT will take every precaution to prevent the users personal data from being lost in the event it must remote wipe a device, it is the users responsibility to take additional precautions, such as backing up email, contacts, etc.
    - The Company reserves the right to disconnect devices or disable services without notification.
    - The user is expected to use his or her devices in an ethical manner.
    - The user assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

2.18 Access to Personal Information

In the course of your role,you may have access to the personal information relating to students, staff, the business of the Company or third parties. You must comply at all times with the following when accessing systems that contain personal or confidential information.

- Only process personal information in so far as required in order to complete the specific task and not for any other reason.
- Not reveal or disclose personal, sensitive or identifiable information to anyone other than the individual for the purpose of your job role.
- Not download any individual's personal information onto personal devices such as USB sticks, phones, cameras etc., nor take any photo of any individual member of staff or student without their express permission.
- Safeguard and protect all personal information from unauthorised or unlawful processing, including (but not limited to) accidental loss, destruction or damage.
- Inform the Company immediately if you have done something (or are asked to do something) infringing the requirements of this Policy even where such action or breach is accidental or inadvertent.
- If you have any doubts about the confidentiality of any information, it must be regarded as confidential unless you are advised otherwise by your supervisor/line manager.

2.19 Monitoring

The Company reserves the right to regularly audit User activity and IT systems to ensure compliance with this and other Company policy. Our tools provide us with the information to monitor your physical location, however we only review this information when required to recover lost devices or investigate Information Security incidents. Access to Company IT systems is provided on condition that users consent to monitoring in accordance with Policy. Your use of Company IT systems constitutes your consent to the monitoring.

3 Compliance

3.1 General

All users of the Company's IT systems, services and equipment are required to read this policy and to agree that they have read, understood and are willing to abide by its contents. The method on how this agreement is presented and accepted is to be explicit.

3.2 Breaches

Any user suspected of any conduct contrary to this Policy must report the conduct to Corporate IT. Breaches of policy compliance may result in disciplinary action being taken against the offender.

3.3 Relevant Legislation

The Company is a global organisation with the responsibility to maintain compliance with the laws within our host nations. All Company users are responsible for aiding the Company In identifying relevant legislation and for complying with all relevant legislation. Users need to be particularly aware of the General Data Protection Regulation (GDPR) and Privacy Act for the Country and region they operate within.

4 Responsibilities

Each of the positions involved in implementing and achieving policy objectives and carrying out procedures are shown here.

Responsibility	CTO	Company IT Gov.	All Users	Company IT Leaders
Approver of Document	A			
Maintenance of Document		A		
Review of Document				C
Understanding of document			R	

R = Responsible, A = Approve, S = Supporting, C = Consulting, I = Informed.

5 Definitions

Unless the contrary intention is expressed in this Policy, the following words (when used in this policy) have the meaning set out below:

Term	Meaning
One Pass Data Erasure	See definition HERE.
BYOD	Bring Your Own Device (abbreviation).
Company	Means Navitas Pty Ltd and its affiliated group companies.
IT Asset	Any device such as a tablet, phone, computer (desktop, laptop), printer, peripherals such as keyboard, montiors and mouse, servers, storage and network equipment.
Website (where relevant)	Means the Company's website where information is available to users and other interested persons or organisations.

6 Review

This Policy is tested and reviewed and any changes to the regulatory compliance requirements, legislation, regulation and guidelines. This review process aims to ensure alignment to appropriate strategic direction and continued relevance to the Company's current and planned operations.

7 Records Management

All records in relation to this document will be managed as follows:

Record type	Owner	Location	Retention	Disposal
Policy	Chief Technology Officer	Electronic	Permanent	N/A