Numatic

ACCEPTABLE USE POLICY

The purpose of this policy is to establish acceptable practices regarding Information Resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

ACCEPTABLE USE POLICY

CONTENTS

ACCEPTABLE USE POLICY

1 PURPOSE

Protecting our business is a responsibility we all share and requires the right balance in giving our people the freedom to succeed whilst enforcing guidelines and policies that ensure that we work safely, securely, and responsibly.

This policy sets out how we manage and handle our IT equipment and data, and the standards that must be observed when using and/or accessing them.

The misuse of Numatic International's IT equipment and data can seriously damage Numatic International's business and reputation, and therefore it is extremely important that all employees (including full time, part time, temporary, work placement), consultants, contractors, sub-contractors, agents who will henceforth be referred to as individual(s), read and understand the policy – as the responsibilities outlined must be followed in full.

Breaches of this policy may be dealt with under the Disciplinary Policy and, in serious cases, could be treated as gross misconduct leading to summary dismissal.

2 INTRODUCTION TO THE POLICY

Numatic International's data is essential to the current and future success of the business. Maintaining the security and availability of Numatic International's data is a necessity and is core to our business.

We are required to ensure that Numatic International data is not at risk through loss or unauthorised modification (whether deliberate or inadvertent) and that the integrity of our data is maintained throughout its lifecycle.

Numatic International has legal, statutory, regulatory and contractual obligations that include information security. Furthermore, we need to demonstrate information security to our customers. Numatic International's information security policies, standards and procedures assist us in achieving these goals. You have an obligation to adhere to these policies, standards and procedures.

Information security is the preservation of the confidentiality, integrity and availability of information:

- Confidentiality – Protecting sensitive or personal information from unauthorised disclosure, both to outsiders, and to employees or contractors who have no requirement to access such information in the course of their duties.
- Integrity – Safeguarding the accuracy and completeness of information and information processing methods, against any unauthorised changes.
- Availability – Ensuring that information and associated services are available to meet Numatic International's business needs.

Information security is required during the whole lifecycle of information based in Numatic International, from the moment it is collected or created, throughout its usage, to ultimate disposal. Appropriate measures need to be applied to ensure that information security is maintained. Information security promotes trust and confidence in Numatic International's services, business practices and IT infrastructure and systems.

The achievement of information security requires a combination of policies, standards, procedures, appropriate organisational structure, physical security considerations, and measures to safeguard the IT network infrastructure and information systems.

If you need assistance on any of the information security requirements contained in this policy, you should seek advice from your line manager or from the IT&DS Infrastructure & Security team.

3 SCOPE

This policy applies to all individuals irrespective of status who have access to Numatic International's data and systems.

It applies to the use of all facilities, equipment and systems that process or store Numatic International's information.

It applies whether the access and use of systems and data, occurs on Numatic International's premises or remotely from any location including, but not limited to, home working.

4 POLICY STATEMENT

Numatic International's policy is that our facilities, equipment, systems and data shall only be used and accessed in acceptable ways that ensure the confidentiality, integrity and availability of the information.

5 ROLES AND RESPONSIBILITIES

- The Head of Infrastructure & Security is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Operational teams shall manage the implementation of any specific requirements detailed in this policy for in house and third-party applications, systems and services.
- Development teams shall ensure that the methods and capabilities as detailed in the policies and standards are detailed as use cases and appropriate capabilities are created within Numatic International's own applications, systems and services to ensure the policies can be applied.
- Line managers are directly responsible for implementing this policy within their functions/departments, and for adherence by all individuals.
- All individuals shall comply with this policy and facilitate its implementation.

6 WHAT IS YOUR RESPONSIBILITY?

You are personally accountable for assisting Numatic International in maintaining the confidentiality, integrity and availability of its information.

All individuals are faced with information security risks and responsibilities daily. Effective security management is about mitigating our risks. From an organisational perspective, this has been achieved through the development of information security policies, standards and procedures, together with complementary information security training and awareness.

Poor information security management can, for example, lead to:

- Leakage and compromise of sensitive information, e.g., personal or commercial information.
- Loss of critical information.
- Fraudulent activities, e.g., identity theft; and
- Failure to comply with legal, statutory, regulatory or contractual requirements.

A direct result of such an occurrence could be that our business, research opportunities and relationships with our customers will suffer. In order to avoid such instances, we shall all take necessary steps to ensure that security is maintained, including the following:

- Ensure that Numatic International's Information Security Policy requirements are always complied with.
- Obtain advice from line managers, or the Information Security team when unsure.
- Request training when needed.
- Complete training when required.
- Report any suspected security incidents as directed by Numatic International; and
- Make recommendations on how we can improve our information security.

Enabling Numatic International to operate in a secure environment requires us all to work as a team towards the same goal of information security.

7 ACCEPTABLE USE OF IT ASSETS

All IT processing facilities and equipment to be used in connection with Numatic International's information shall be formally configured and authorised by the IT&DS Department and approved by relevant information system owners or line managers before such use.

The IT&DS Department shall use and maintain a documented list of approved products, used for selecting IT equipment, and shall manage an inventory of all acquired IT assets. This includes recording of personnel authorised to use the IT assets, and any labelling requirements for the IT assets. All IT assets shall be returned to the IT&DS Department when they are no longer required – this will help maintain the IT asset inventory.

Individuals can only use personally owned devices for Numatic International's business purposes subject to formal authorisation.

All the IT equipment, devices and software that you have been assigned remains the property of Numatic International. You have an obligation to ensure that this equipment and software is safeguarded and only used as intended by Numatic International:

- You shall not remove any IT equipment from Numatic International's premises without the authorisation of the IT&DS Department and relevant information system owners or line managers.
- You shall always take care of IT equipment allocated for your use and treat it as if it is your own.
- You shall protect your IT equipment against theft and unauthorised access.
- You shall not store any access control device with equipment or devices which are reliant on the same device for multi-factor authentication.
- You shall not expose your IT equipment to any environmental hazard, such as extremes of temperature.
- You shall not install any unauthorised or unlicensed software on your IT equipment. If you require any software for your work, you shall get approval from your line manager and the IT&DS Service Desk.
- You shall not modify your IT equipment in any way; this includes any amendments to the hardware and software configuration.
- You shall not install any unauthorised tunnelling or peer-to-peer software or service.
- You shall not install any monitoring avoidance software or service.
- You shall always report any IT problems to the IT&DS Service Desk.

Specific acceptable use requirements in connection with protection against malicious code such as viruses and spyware, secure use of e-mail and Internet access, and protection of copyright materials are documented below.

Numatic International provides primary access to its systems and IT equipment for business use but recognises that there are times when you will need to complete personal tasks online, and reasonable personal use of equipment is permitted.

When you use Numatic International equipment assigned to you for personal and/or business matters, you shall ensure that you do not:

- Violate any laws, professional standards or Numatic International policies.
- Create the appearance of impropriety on the part of Numatic International.
- Violate or infringe upon the intellectual property rights and property of others.
- Put the rights and property of Numatic International or its clients at risk.
- Compromise, embarrass or bring into disrepute Numatic International's brand, reputation or relationships with its clients.
- Utilise Numatic International identities, including business e-mail address(es), for personal accounts or services.

- Impede any Numatic International business activity, including your own productivity.
- Impersonate others or position yourself as an authorised spokesperson for Numatic International in online forums or social media without prior written approval.

If you are using Numatic International equipment for personal use (such as conducting online banking, booking a holiday or shopping) you do so at your own risk, and, if you have any concerns about the security of Numatic International's equipment, you shall use alternative means for conducting your personal business. Wi-Fi access is provided such that you can use your own device for personal use. (A Wi-Fi guest network may also be available for visitors).

8 SITE SECURITY

Physical security involves protecting Numatic International's premises, individuals, information and IT assets from unauthorised physical access and physical security threats, e.g., fire, invasion, theft and wilful damage. All individuals shall support Numatic International's site security requirements. Individuals shall not allow unauthorised physical access into Numatic International's offices, computer rooms and sensitive areas, and shall report physical security threats to Facilities Management as soon as possible using Numatic International's standard reporting procedures.

If you are allocated with keys or other controls (such as electronic key fobs or swipe cards) for access to Numatic International's offices or facilities, ensure you keep them in a secure location, and protected from unauthorised access. If they are lost or stolen, you shall immediately report this to your line manger..

Do not allow anyone to 'tailgate' when you are entering a perimeter gate, door of a building or a secure area. If you are suspicious of any person, tactfully challenge them to ensure that they have a legitimate reason to be there and have authorised access. Unauthorised personnel shall not be permitted to enter a building or a secure area and shall never be unescorted.

Visitors, for whom you are responsible, shall always report to the security office, identify themselves, be provided with a visitor's badge, be always escorted within Numatic International's offices (unless otherwise authorised), and shall return their visitor's badge to the security office before leaving Numatic International's premises, even if temporarily.

9 REMOVAL OF PROPERTY AND SECURITY OF EQUIPMENT OFF-PREMISES

Other than laptops and mobile devices assigned to individuals for their permanent use, Numatic International's IT equipment shall only be taken off-site following formal authorisation by the IT&DS Department, whilst Numatic International's information shall only be taken off-site following formal authorisation from the relevant information owner or line manager.

All individuals are responsible for protecting authorised off-site equipment (allocated to them) against physical security threats and unauthorised access. See section 0below for more detail.

Individuals shall always ensure that off-site Numatic International information is securely handled in line with the Information Classification and Handling Policy.

10 SECURE DISPOSAL AND RE-USE OF EQUIPMENT

All Numatic International's information and software shall be securely wiped from Numatic International's IT equipment before disposal or re-use of the equipment. All equipment intended for disposal and re-use shall be returned to the IT&DS Department, who shall securely wipe Numatic International's information and software from it, using established procedures.

Where data cannot be securely wiped, the media shall be removed and retained , or securely destroyed to ensure the information cannot be later retrieved.

11 PROTECTION AGAINST MALWARE

Computer viruses, spyware, remote access Trojans, ransomware and other forms of malicious code (malware) exploit vulnerabilities in software programs and can cause loss and damage to Numatic International's information, software and IT equipment or unauthorised access to Numatic International systems and services.

Numatic International uses a variety of products, e.g., monitoring, anti-virus and software security patches, network-based scanning and firewalls which are frequently updated to reduce the threat from viruses and other malicious code. Numatic International's PCs and laptops are also protected by these controls. You shall not change or remove these controls on your Numatic International PC or laptop, otherwise Numatic International's IT network, systems and information will become more vulnerable to the threat from viruses and other malicious code.

In addition to these controls, Numatic International is also dependent on individuals, who shall remain vigilant to protect Numatic International from malicious code. You shall ensure that:

- You do not introduce a virus or malicious code into the corporate network, by downloading unauthorised or suspect software from the Internet or from computer media, e.g., DVDs, CDs and USB storage or smart devices onto your PC, laptop or any Numatic International system or service.
- All software and data which originates from outside Numatic International shall be checked for viruses and malicious software prior to it being opened or used – if you need help, contact the IT&DS Service Desk.
- If you are suspicious of a virus or malicious code, you shall stop using your PC or laptop immediately and contact the IT&DS Service Desk.
- If you receive a suspicious e-mail, you shall not open or preview it, or the attachment or any hypertext link, as this may well activate a virus or other form of malicious code. Immediately contact the IT&DS Service Desk.

There may also be 'hoax' virus messages in circulation which are not actually viruses at all, but plain e-mail messages asking you to take some sort of action, such as deleting files on your computer and forwarding the message which then due to the number sent become 'viral' themselves. These messages themselves are not infected with a virus, and are spread by playing on people's fears, and fooling them into following the instructions. If you receive a message warning you of a virus, you shall immediately contact the IT&DS Service Desk.

12 SECURE HANDLING OF MEDIA AND DOCUMENTATION

Care shall be taken to protect all documentation and computer media, e.g., DVDs, CDs and USB storage devices or smart devices containing sensitive and critical information, and measures shall be taken to ensure secure storage, transit, copying, reuse and disposal of computer media and documentation.

When exchanging information within Numatic International or between Numatic International and other organisations, it is vital to assess the sensitivity of the information and handle it appropriately.

The use of USB devices poses a risk to Numatic International in respect of loss of data and other intellectual property, and potential introduction of malware. Numatic International has facilities that allow the secure exchange of information without the use of USB drives, which are preferred for information exchange. Contact the IT&DS Service Desk for further information.

In order to mitigate the associated risk, Numatic International's policy regarding the use of USB devices is as follows:

- Individuals shall only use encrypted USB devices procured by the IT&DS Department.
- All USB devices shall be scanned for malware before use.
- Any USB devices provided by third parties to transfer data to Numatic International shall be passed on to the IT&DS Department for malware scanning and (when required) encryption before use.
- The IT&DS Department shall have an adequate supply of encrypted USB devices to swap unencrypted devices for encrypted ones where required.

- Numatic International's laptops and desktop PCs shall have their USB ports configured to read/write data only from/to suitably encrypted USB devices.
- The use of USB devices to transfer information to third parties, or between Numatic International offices, is discouraged; but, where that use is justifiable and accepted, it shall be ensured that passwords are communicated to the recipient(s) in a secure way, using a separate channel – never written on or in any way attached to the device.
- Numatic International provides power sources which can be used to charge USB devices. Numatic International laptops shall not be used as a power source for personal devices.
- Individuals shall not sync their personal devices with a Numatic International laptop or another device and shall be aware that any data on Numatic International devices will be inspected which may result in data being relocated or removed.
- Individuals shall only backup Numatic International information to approved products and/or services.

When dealing with printed documents, always ensure that you are aware of their security classification and handling requirements. Sensitive documents shall not be left or reviewed in public or on public transport, or left unattended on desks, printers, facsimiles and other equipment where they are vulnerable to unauthorised access and theft.

You shall always lock sensitive computer media and documents away when left unattended.

13 STORAGE OF INFORMATION IN THE CLOUD

Users shall only store or share Numatic International information in the Cloud using products and services approved by Numatic International. The IT&DS Department shall be consulted before any attempt to store information with a Cloud Service Provider that is not approved by Numatic International.

Individuals must be aware that some financial and personal Numatic International information may be subject to local legislation, including but not limited to data protection legislation, where cloud services used must restrict the storage of Numatic International or other information to a particular geographic region. Contact the IT&DS Service Desk for more information or clarification.

14 E-MAIL/MESSAGING SECURITY AND SECURE INTERNET ACCESS

Messaging system (Including but not limited to instant messaging and E-mail) and Internet are provided to you as a means of improving your communications, collaboration, knowledge and effectiveness at work. Numatic International's messaging and Internet facilities are intended for business use. All usage of Numatic International's messaging and Internet facilities is treated as the property of Numatic International and shall not be regarded as private.

Numatic International messaging systems may not be used for exchange of inappropriate (including pornographic, obscene, offensive, racist, defamatory, harassing or intimidating) content, to facilitate personal financial gain, or for political purposes.

Individuals shall be aware that Numatic International reserves the right to use monitoring tools to enforce Numatic International policies, retain information from and about messages exchanged, and will produce periodic reports detailing use of all messaging and Internet access facilities.

Use of messaging systems and Internet access introduces security threats such as malicious code attacks, e.g., viruses, unsolicited or undesirable e-mails, attempt to initiate financial transactions, fraudulent attempts to acquire sensitive information such as research, passwords and payment card details, unauthorised content, and breaches of legislation, e.g., computer misuse and copyright legislation. If you accidentally access any material which is not permitted, you shall report this to your line manager and the IT&DS Service Desk immediately.

E-mail is an insecure method of communication and messages may well be read by those who have no authority to do so. Before sending information via e-mail, you shall first assess the handling requirements of that information and if e-mail is the correct means to exchange data.

Numatic International e-mail may not be auto forwarded to a third party or public e-mail system unless there is an approved documented business need.

15 INFORMATION SECURITY IN CONVERSATIONS AND WITH THE USE OF TELEPHONES, FACSIMILES AND RECORDING EQUIPMENT

Due care shall be taken when using telephones, voicemail, conferencing, answering machines, facsimiles and recording equipment (e.g., photographic, video and audio equipment) to ensure the protection of sensitive information. Individuals shall comply with the Data Protection Policy.

It is important that before you conduct a telephone conversation in an open plan office area or outside of Numatic International's premises, you shall consider the nature of the topic you are about to discuss. If the conversation is of a sensitive nature, you shall ensure that there is no possibility of eavesdropping. Conversations which discuss any non-public Numatic International information, strategy, financial or customer specific details shall not be held on public transport or in public areas. Remember to always be aware of who is around you when holding a confidential conversation. In addition, messages containing sensitive Numatic International information shall not be left on voicemail and answering machines.

When sending or receiving sensitive information by facsimile, you shall ensure that the information is not compromised. Always check the recipient facsimile number to ensure that it is correct before sending information. Ensure that the information is collected immediately from the facsimile. Ensure that all sensitive information sent by facsimile is destroyed when no longer needed, by cross-cut shredding or by using confidential waste bins provided by Numatic International.

16 USER IDENTIFICATION, ACCESS AND MONITORING

You shall only access and use Numatic International's IT network, systems and applications if you are authorised to do so. If you are granted access, it is so that you can perform your duties efficiently.

You shall remember that access has been granted for your sole use by means of a unique user account and password. This applies to the different user accounts that may be granted to you for access to Numatic International's network, information systems and applications. You shall not give details of your user account and password to anyone, including your line manager; you shall not share any user account allocated to you with anyone else. Numatic International (within its legal rights) can track the activities of each user via their user account and identify exactly what information and systems or services they have accessed and what actions have been taken. If it is your user account that is logged as attempting an unauthorised or illegal action, you may be held responsible. It is in your interests to ensure that you always safeguard your user account and password details.

In order the ensure compliance with legislation, regulations, contracts and its information security policies, Numatic International reserves the right to monitor user activities and data flows.

17 PASSWORD SECURITY

Passwords are a key control to maintain information security. They help us ensure that only authorised persons have access to Numatic International's IT network and systems. For your password to be effective and remain secure, you shall comply with the following simple rules.

Passwords shall be always kept confidential and shall not be disclosed to or shared with anyone, not even your line manager or the IT&DS Department. Shall someone require approved access to your information (e.g., long term absence) it can be shared through other means. Contact the IT&DS Service Desk for more information.

Ensure that your password is memorable, so that you do not need to write it down or electronically store it. Written down passwords are strongly discouraged. Electronically stored passwords are strongly discouraged, unless the passwords are secured via an IT solution that is approved by the IT&DS Department. Online text or documents for passwords shall never be used.

Ensure that your password is difficult for others to guess. When creating your password, you shall always use good password practice:

- DO:
- Follow the password complexity rules prescribed in the Password Policy.

- When using smart devices, ensure any PIN or shape drawn/tapped is not obvious, (e.g.: square, single right angle, etc.).
- DON'T (individually or as a combination of):
- Use your user ID.
- Use names (e.g., your name, or the names of your partner, children and heroes, or place names).
- Use information, which is well known to others, or could be gleamed through social media (e.g.: hobbies, brands, holiday resort destinations, family/pet names, celebrities).
- Use dates (e.g., birthdays, anniversaries, other memorable, recurring or dates associated with significant/major events).
- Use words that people can associate you with (e.g., birthplace, home address, Numatic International's address, sporting team(s)).
- Use words from any dictionary (e.g.: local and any second languages you may use).
- Use successive passwords that follow an easily predictable pattern (e.g.: [Password]01, [Password]02, [Password]A, [Password]B).
- Use the 'Save/Remember Password' feature that is provided in some applications.

Ensure that you are not overlooked when typing your password. If your password is disclosed to anyone or compromised in any way, you shall change your password immediately.

Always contact the IT&DS Service Desk to discuss any issues regarding your password.

18 CLEAR DESK AND CLEAR SCREEN

Measures shall be taken to adequately protect against unauthorised physical access to Numatic International's information hosted on PCs, laptops, handheld devices (e.g., tablets, mobile telephones, and digital cameras), computer media (e.g., DVDs, CDs and USB storage devices), and paper documentation.

All individuals shall ensure that access to their user accounts is password protected when their computer devices are left unattended, even for a small amount of time, e.g., 1 minute. This can be done by following these simple steps:

- Press Ctrl, Alt, Delete buttons together.
- A dialog box will appear. Within this, click on the 'Lock This Computer' option.
- Alternatively, press the 'Windows' button and 'L'.

All individuals shall ensure that all mobile equipment, e.g., laptops and tablets, sensitive computer media and sensitive documentation are not left unattended and insecure, but are appropriately stored in locked areas or facilities, e.g., locked cabinets, and that access to relevant keys is controlled.

At the end of a working day, you shall:

- Logoff from and shut down your PC or laptop.
- Clear your desk and lock all sensitive computer media and documents away in a drawer or cabinet with suitably restricted access.
- If you are a user of a laptop or handheld device, and you are not taking it with you, lock it away in a drawer or cabinet with suitably restricted access.

19 REMOTE WORKING

Remote workers include:

- Mobile workers: all users who use Numatic International's information and information processing facilities whilst not located on Numatic International's premises, e.g., workers who are in other organisations' offices, in hotels and conferences, and travelling workers.
- Home workers: users who have been authorised to use Numatic International's information and information processing facilities whilst based at home, or larger groups of Numatic International employees required to work from home during exceptional periods of disruption or mandatory changes to working practices.

Laptops, mobile phones, tablets, and other such portable equipment are expensive and valuable assets that are highly desirable, particularly to the opportunist thief. Loss of such equipment not only has an obvious financial implication but may also compromise the information that is on the equipment itself. Exposure of this information could result in breaches of Numatic International's legal, regulatory, statutory and contractual obligations, and damage to Numatic International's reputation. For example, the loss of a laptop which holds a file containing personal details of employees is likely to result in contravention of data protection legislation. This could lead to Numatic International, and possibly the individual concerned, facing a fine or in extreme circumstances imprisonment.

All policies and procedures that apply to individuals based at Numatic International's offices also apply to remote workers. As your remote working environment is not fully controlled by Numatic International, it is your responsibility as a mobile or home worker to ensure that appropriate security controls are implemented to protect Numatic International's information and IT assets.

All remote workers shall comply with the Remote Working Policy. Amongst other considerations, this policy addresses:

- Physical protection of Numatic International's information and information processing facilities.
- Secure remote access to Numatic International's IT network and systems.
- Regular backups of Numatic International's information.
- Any Numatic International device used at home is not provided as a replacement for a home or individual owned device and shall not be considered a family computer or device.
- As per this policy only Numatic International licensed software shall be installed on Numatic International devices.
- Use of an Numatic International device does not make Numatic International accountable or responsible for any personal losses, financial or otherwise, incurred using that device due to malware, or data loss.

More information can be obtained from the Remote Working Policy.

20 REPORTING INFORMATION SECURITY INCIDENTS

For Numatic International to be able to manage and deal with information security incidents successfully, they shall be captured and logged.

If you suspect or have knowledge of an information security incident or event, or a breach of Numatic International's information security policies or procedures, or a software malfunction, or a security weakness in any Numatic International building, network or information system, you shall report the concern immediately to the IT&DS Service Desk.

Examples of an information security incident include:

- Compromise of personal or sensitive information, e.g., commercial data or personal data.
- Malware being discovered on one or more devices.

- Physical damage to Numatic International equipment that stores, retrieves, transmits or manipulates information.
- Events that significantly disrupt the availability of Numatic International resources.
- Unauthorised use of another user's profile (masquerading of user identity).
- Divulging a password to another user without authority.
- Improper use of email or the Internet, e.g., downloading or distribution of unauthorised software, and non-business-related activities that rise above acceptable use.
- Unauthorised copying and/or distribution of Numatic International information.
- Damaging or impairing the functioning of Numatic International resources in a manner that may impact information security.
- Unauthorised access to Numatic International resources from internal or external sources.
- Theft of Numatic International resources.

Remember, it is vital that you report all confirmed or suspected information security incidents. Withholding information or failing to report an incident could result in you being held personally liable. Individuals shall not attempt to deal with the information security incident (other than reporting the incident), otherwise they may become involved in disciplinary or legal action.

If in doubt, please contact the Head of Infrastructure & Security or your line manager for advice.

21 INTELLECTUAL PROPERTY RIGHTS (IPR) AND COPYRIGHT LEGISLATION

All individuals shall observe intellectual property rights and copyright legislation. The main purpose of such legislation is to protect the developer of the information, software, or other original material, and prevent its improper use. If it is necessary to make copies of such materials, the express permission of the copyright owner shall be granted first. In addition, a user licence is normally required to use copyrighted software.

Only authorised, legal software shall be stored and processed on Numatic International's IT network and systems. You shall not install or copy any software on Numatic International's IT equipment, e.g., music files. If you require any software for your work, you shall firstly consult your line manager and the IT&DS Service Desk.

Software developed by individuals whilst working for Numatic International is the intellectual property of Numatic International, and it shall not be used for any other purpose outside of Numatic International's authorised business requirements.

Users shall not copy and distribute hardcopy documentation that is copyright protected without authorisation by relevant Numatic International information owners and line managers.

22 DATA PROTECTION LEGISLATION AND PRIVACY OF PERSONAL INFORMATION

Data protection regulations, including the General Data Protection Regulation (GDPR), are concerned with the direct use of personal information, whether that information is a manual record or processed on a computer system. Data protection legislation and regulations apply to all types of personal information; this includes information which may not be thought to be confidential.

Personal data means data that relates to a living person who can be identified from that data, or a combination of that data and other information which is in the possession of Numatic International. It also includes any expression of opinion about the individual.

The GDPR has data handling principles, all of which shall be adhered to when handling personal information. The principles include specific requirements that address the security aspects of handling personal information.

If Numatic International fails to abide by data protection legislation and regulations, it could be heavily fined, and its business operations could be negatively impacted. Personal liability is also imposed, so if an employee is found to be contravening data protection requirements, he/she could be prosecuted too.

All individuals shall comply with data protection legislation and regulations, and the Data Protection Policy. If you are unsure about any data protection requirement, contact the Data Protection Officer (DPO) for assistance. It is your responsibility to be familiar with and to adhere to the requirements of data protection legislation and regulations.

More information can be obtained from the Data Protection Policy.

23 COMPUTER MISUSE LEGISLATION

All users shall comply with applicable computer misuse legislation. Such legislation, generally aimed at computer 'hacking', specifies offences for any unauthorised access to internal organisational systems.

Computer misuse legislation generally defines as criminal acts:

- Unauthorised access.
- Unauthorised access with intent to commit a further serious offence.
- Unauthorised modification of computer material.

Individuals shall only access systems they are authorised to use. It is an offence to knowingly gain unauthorised access to a computer system, and this could result in a fine or imprisonment.

24 POLICY REVIEW DATE

This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.