Appendix I: Use of ICT accounts, devices and tools

Use of devices

This policy is established to minimize the risk of loss or exposure of sensitive information owned by Neways as well as reducing exposure to external sources of malware and virus exploit within Neways. This policy applies to all Neways Employees using Neways devices.

All user devices (smartphones, tablets, convertible laptops, and various other personal computing devices) owned by Neways or owned by Employees, that have access to Neways systems and applications are governed by this policy. Applications, including cloud storage software used by Employees on their own personal devices are also subject to this policy. The following general procedures and protocols apply to the use of these devices.

- User devices must be protected with a password, required at power on and when returning out of idle state;
- All data stored on devices shall be encrypted;
- Wireless encrypted security and access protocols shall be used with all wireless network connections;
- User shall verify that the network he/she uses is secure. If you cannot verify don’t use it;
- User shall immediately report any loss of stolen in accordance with the data breach protocol as laid down in the internal privacy policy;
- User shall immediately report any unauthorized access to a Neways device or – data in accordance with the data breach protocol as laid down in the internal privacy policy;
- Users shall make use of the Neways corporate email account when sending or receiving Neways data and correspondence;
- User devices shall not be “rooted” or have unauthorized software/firmware installed;
- Users shall not deploy illegal content or pirated software onto any user device;
- User devices shall be kept up-to-date.
- Neways expects Employees to take care of devices and use these properly.

Use of software and copyright protected material

The use of software that has not been purchased by Neways, nor on behalf of Neways is not permitted. Any media received from customers or suppliers should only contain software related to the business of Neways. Moreover, information carriers must first be examined for viruses before the software can be installed. If in doubt always contact the ICT department.

Neways respects the copyright of anyone involved in the creation and distribution of copyrighted works such as music, films, computer programs, video games and other literary, artistic and scientific works. Employees of Neways are not allowed to download, offer or store illegal copies of copyright protected work in any form whatsoever, using Neways resources such as ICT systems and / or storage media. All files, activities or goods that are found to be in violation of this policy will be immediately removed, suspended and/or forfeited.

Use of removable media

Removable media takes many forms today and is personal, removable and portable which introduces risk into the organization whenever it is used to store sensitive information. Aside from the chance for loss and theft, removable media format storage is a well-known source of malware infections and has been directly tied to the loss of information.

For the purposes of definition, the following items shall fall under the category of removable media, but are not limited: Flash (Jump) Drives, flash memory storage, SD storage, removable fixed drives, R/W Compact Disk or DVD media, USB remote storage devices.

Removable media storage of any type are not allowed in any form or function within the Neways operational environment. Personal storage devices shall not be used for storage of any Neways information and neither be used with Neways hardware. Exceptions to this policy shall be considered only in unique and rare cases and are subject to management approval.

Usage of network accounts

The following rules and behaviour must be respected by all Neways Electronics employees and ICT users:

- Each individual user is responsible for the correct use of their personal accounts and passwords;
- Accounts and passwords are confidential and personal, and must be kept secret by the user;
- Passwords shall not be shared, written down or stored in a readable manner;
- Entering a password shall be done in such a way that others cannot observe it;
- A password must be difficult to guess. Not allowed are person or pet names, user names, date of birth, license plates, simple combinations of repetitive characters etc.;
- When a password is compromised it must be changed immediately;
- When a password is abused it must be reported to Corporate ICT immediately;
- Users who received permissions for installing and adjusting software themselves are responsible for their workspace, local software and local data (including backup). If unsolvable problems arise, as a result of which the workplace needs to be replaced, the user is responsible for reinstallation of the software. Applications shall be kept up-to-date.

The following activities are expressly prohibited:

- The introduction of network monitoring or password detecting software on any Neways user machine or part of the network;
- Seeking to gain access to restricted areas of the network;
- The introduction of any form of computer virus;
- Other hacking activities;
- Knowingly seeking to access data which you know, or ought to know, to be confidential and therefore would constitute unauthorized access;

Use of internet, social media and email

The policy is intended to help employees of Neways make appropriate decisions about the use of internet, social media and e-mail. It applies to use of internet, social media and e-mail for business purposes as well as personal use that affects our business in any way.

Use of the internet and email

Limited personal use of the internet and of email at work is acceptable provided it does not interfere with or impede your normal duties.

- Users may access non-business related sites, but are personally responsible for what they view.
- You should not engage in any activity which is illegal, offensive or likely to have negative repercussions for Neways;
- Always ensure that Neways is neither embarrassed nor liable in any way by your use of the internet.
- The auto-forwarding functionality within the Neways email system should not be used to forward work emails to private accounts;
- Attachments to emails should only be used when strictly necessary. When hyperlinks are available these should be used. Large files should be compressed and key information from small files may be cut and pasted into the email itself. It is Neways policy that no attachment should exceed 10 Mb in size;
- Remember that a phone call or face to face discussion may often be more appropriate than an email, bearing in mind that an email may be misinterpreted or lead to a chain reaction. Also, consider carefully who really needs to be copied on emails. Unnecessary email can be a major distraction;
- Be aware of malicious / spam email. Do not follow up instructions from these emails (e.g. provide personal / business information) Inform the ICT Servicedesk in case of malicious email;
- When a user leaves Neways, the email archive will be deleted together with the account, after 90 days.

You may not upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- Are or might be considered to be indecent, obscene or contain profanity;
- Are or might be offensive or abusive in that the context is or can be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful;
- Encourage or promote activities which make unproductive use of your time;
- Encourage or promote activities which would, if conducted, be illegal or unlawful;
- Involve activities outside the scope of your responsibilities – for example, unauthorized selling/advertising of goods and services.

Use of work related social media

Only Neways Corporate communications and HR departments are permitted to post material on social media websites in the company's name and behalf.

Any employee involved in the organisation's social media activities must remember that they are representing the organisation, use the same precautions as they would with any other communication and adhere to the following rules:

- Ensure that the purpose and benefit for the organisation is clear;
- Ensure the content is checked before it is published. Content on the business performance can only be released by Board of Directors. This can relate to financial reporting or restructuring and organizational changes, but is not limited to.

Personal use of social media

Personal use of social media in the workplace is permitted, subject to certain conditions, as detailed below;

- It must not be abused or overused and Neways reserves the right to withdraw permission at any time;
- It must not involve unprofessional or inappropriate content;
- It must not interfere with your employment responsibilities or productivity;
- Its use must be minimal and take place substantially outside of normal working hours, for example during breaks and lunchtime.

General rules for social media use

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules. The same rules would also apply when using social media outside of work:

- Do not post or forward a link to any abusive, discriminatory, harassing, derogatory, defamatory or inappropriate content. This includes potentially offensive or derogatory remarks about any other individual;
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, do not share it with social media;
- Do not post material in breach of copyright or other intellectual property rights;
- Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of Neways;
- You are personally responsible for content you publish – be aware that it will be public for many years;
- Do not post anything that your colleagues or our customers, clients, business partners, suppliers or vendors would find offensive, insulting, obscene and/or discriminatory;
- Do use privacy settings where appropriate but bear in mind that even comments in a restricted environment may be passed on;

- If you are concerned or uncertain about the appropriateness of any statement or posting, refrain from posting it.

Monitoring of internet, email and social media use

Neways is ultimately responsible for all business communications and will, as far as reasonably possible and appropriate, respect your privacy and autonomy while working. Neways may monitor your business communications for reasons which include:

- providing evidence of business transactions;
- ensuring that Neways business procedures, policies and contracts with Employees are adhered to;
- complying with legal obligations;
- monitoring standards of service;
- preventing or detecting unauthorized use of Neways communications systems;
- maintaining the effective operation of Neways communications systems.

Neways will monitor email and internet traffic data (such as sender, receiver, subject; non-business attachments to email, domain names of websites visited, duration of visits, and files downloaded from the internet) for the purposes as described above. You need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using Neways devices you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

Sometimes it is necessary for Neways to access your business communications during your absence, such as in case of long illness or holiday periods. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of the Corporate Head of HR authorized to grant such access.

All incoming email are scanned by Neways using virus checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments.