IT & Cyber Security Policy

1 Statement of Policy

1.1 Nobisco Limited (the Company) wishes to ensure that it's data and information is help securely at all times. To do that the Company sets out expectations for all workers, employees, consultants and agency workers that must be complied with.

1.2 The Company may at times legally monitor IT and electronic activity of its workers. This might include:

- opening mail or email
- use of automated software to check email
- checking phone logs or recording phone calls
- checking logs of websites visited

1.3 Data protection law sets out rules about the circumstances and the way in which monitoring can be carried out and further information is found in the Monitoring at Work Policy.

1.4 It is the responsibility of all workers to conduct themselves professionally with respect, honesty and integrity whilst using electronic communications and to safeguard Company information by understanding and complying with this policy, the Social Media policy, the Data Protection and Data Security Policy and other related policies.

2 IT use

2.1 Unauthorised access of any computer belonging to the Company using another person's password is not permitted.

2.2 No employee should share their password with a colleague

2.3 Do use at least eight characters of lowercase and uppercase letters, numbers, and symbols in your password.

2.4 Strong passwords are easy to remember but hard to guess. Iam:)2b29! — This has 10 characters and says, "I am happy to be 29!". Try short codes, sentences or phrases. 2B-or-Not_2b? —This one says: "To be or not to be?"

2.5 If the password is shared with IT for IT issues only, then the password must be changed once the work is completed.

2.6 You must not disclose confidential information over electronic communication and must always keep all sensitive Company information confidential

2.7 All software is the property of the Company and subject to the Software vendors licencing agreements. Any copying of software is prohibited. The use of pirate software on our computers is also prohibited.

2.8 Virus protection is installed on all computers and all files and emails are virus checked prior to use/opening. If you receive an email you are not expecting from a source you are unfamiliar with please disregard the email immediately and alert your colleagues and a Director, to ensure everyone takes the same action to avoid a suspected virus.

2.9 The Company reserves the right to access all emails sent or received on behalf of the Business at any time.

2.10 All email and telephone contacts are the property of the Company in their entirety, including when generated on remote access systems.

2.11 All devices and equipment including but not limited to mobile phones, desk phones, mobile tablets, laptops, scanners and other electronic equipment are subject to the IT, Internet usage and Social media policies in their entirety. Desk phones are provided for business use only, except in emergency personal situations.

3 Internet use

3.1 You are expected to use your common sense and judgement to ensure safety and confidentiality during internet use.

3.2 Access to the internet is there to support business needs and you are expected to refrain from personal use except during break periods. Adherence to this policy is always expected during personal use.

3.3 The Company will review internet usage to ensure Employees are abiding by this policy.

4 Social Media: please refer to the Company Social Media Policy

5 Cyber risk

5.1 The term “cyber risk” relates to a loss due to either technical infrastructure (e.g. servers, databases) or the use of technology inside an organisation. This loss can take many forms, from a hacker draining a bank account to an employee accidentally exposing private data to site visitor.

5.2 All workers and employees must be alert to the potential risks to the Company or cyber security breaches that may include any of the following:

- Ransomware: a computer program planted in a company’s computer system that effectively blocks the company from accessing it. The perpetrators then demand a ransom to restore access to the data.

- Credential-harvesting malware that targets smartphones and their stored data. For example financial information and personal information.
- Social engineering that involves cybercriminals finding sensitive information from companies by posing as representatives of legitimate organisations i.e. the companies bank. Cybercriminals will typically make these requests using an email that contains official letterhead to help make the email appear legitimate.
- Threats associated with outsourcing and supply chain who have access to Company information.
- Personally identifiable information that includes basic information such as a person's name, address and birth date that can be enough to commit a crime.

5.3 All employees must be extremely careful when responding to emails or telephone calls that ask for information. Suspicious emails should be referred to the IT department. Any telephone call that requests a payment or the release of personal information must eb checked for authenticity.

5.4 **IF IN DOUBT, DO NOT DIVULGE INFORMATION**

6 Misuse of internet and electronic communication

6.1 Any worker, employee, consultant or agency worker who breaches this policy will be subject to the disciplinary process.

6.2 For clarity examples of misusing the internet or any other electronic communication incudes:

- Sending messages or emails which could be interpreted as harassment or bullying as defined under the bullying and harassment policies
- Sending or posting threatening, offensive, malicious or libellous messages
- Forging or attempting to forge email messages
- Creating or sending 'chain letters' through email
- Revealing confidential or non-confidential Company information to any sites or commenting on business matters
- Reading, deleting or modifying colleagues' email without their permission
- Violating your obligations regarding confidentiality, IPR or trade secrets
- Copying business information on to private devices or for use off site
- Accessing offensive or immoral websites
- Supporting or engaging in illegal activities or using business systems for personal gain or purposes unrelated to the Business's business
- Breaching any of the Company policies or guidelines.

6.3 If you suspect or have evidence of any abuse of this policy, you must report this to a Director or the MD immediately. Any suspicion of an insured loss must be reported to the insurers via the MD immediately.