* * * Sirius Acceptable Use of IT Policy * * *

CONTENTS

Clause

DEFINITIONS

Sirius Group ("**We**" or "**Group**") - the group of companies from Sirius Real Estate Limited (parent company, Guernsey registered) through to all subsidiaries, including all Dutch, UK, Cypriot as well as German subsidiaries, specifically: Sirius Facilities (UK) Limited, Sirius Facilities GmbH, BizSpace Limited, BizSpace II Limited, M25 Business Centres Limited, Curris Facilities & Utilities Management GmbH, LB2 Catering and Services GmbH, DDS Conferencing and Catering GmbH and SFG Nova Construction and Services GmbH and Sirius Renewable Energy GmbH.

1. Overview

1.1 Sirius IT’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Sirius’s established culture of openness, trust and integrity. Sirius is committed to protecting Sirius's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.2 Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, as well as access to services, software, operating systems, storage media, cloud services, network accounts providing electronic mail, WWW browsing access using Sirius networks are the property of Sirius. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

1.3 Effective security is a team effort involving the participation and support of every Sirius employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, software and services at Sirius. These rules are in place to protect the employee and Sirius. Inappropriate use exposes Sirius to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

1.3 This policy applies to the use of information, electronic and computing devices, and network resources to conduct Sirius’s business or interact with internal networks and business systems, whether owned or leased by Sirius, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Sirius and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Sirius’s policies and standards, and local laws and regulations.

1.2 This policy applies to employees, contractors, consultants, temporary workers, and other workers at Sirius, including all personnel affiliated with third parties. This policy applies to all equipment, software and services that is owned or leased by Sirius.

4. General Use and Ownership

4.1 Sirius proprietary information stored on electronic and computing devices whether owned or leased by Sirius, the employee or a third party, remains the sole property of Sirius. You must ensure through legal or technical means that proprietary information is protected.

4.2 You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Sirius's proprietary information, or any Sirius-issued devices.

4.3 You may access, use or share Sirius proprietary information only to the extent it is authorised and necessary to fulfill your assigned job duties.

4.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

4.5 For security and network maintenance purposes, authorised individuals within Sirius may monitor equipment, systems and network traffic at any time.

4.6 Sirius reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5. Security and Proprietary Information

5.1 Personal devices may not be connected to the Sirius network without prior permission from the IT Director. The Head of Group Technology, Simon Mason, can be contacted as follows: smason@siriusfacilities.com.

5.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

5.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

5.4 Postings by employees from a Sirius email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Sirius, unless posting is in the course of business duties.

5.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

6. Unacceptable Use

6.1 The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

6.2 Under no circumstances is an employee of Sirius authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Sirius-owned resources.

6.3 The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

6.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Sirius.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Sirius or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Sirius business, even if you have authorised access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Sirius computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Sirius account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the IT Director is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Sirius network. Honeypots and honeynets are computer systems or network components that are specifically designed to attract attackers. They can be used to study attack methods, divert attention from other systems or set a trap for hackers.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Sirius employees to parties outside Sirius.
- Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any corporate or non-corporate computer.
- Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.
- Disclosing any corporate information that is not otherwise public.
- Accessing or storing any offensive material on any system owned by Sirius or any system connected to the Sirius network.
- Removing, copying or transferring any data owned by Sirius to unencrypted removable media, or to any storage facility or email account not owned by Sirius. This includes online storage or archiving services such as provided by Dropbox, Microsoft, Amazon, and includes any system or mobile device not owned by Sirius.

7. E-Mail and Communication Activities

7.1 When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

7.2 The sending of unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to persons who have not expressly requested this material (e-mail spam), is prohibited.

7.3 Any form of harassment by e-mail, telephone or paging, whether by language, frequency or volume of messages, is prohibited.

7.4 Unauthorised use, or forging, of email header information is prohibited.

7.5 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is prohibited.

7.6 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

7.7 The use of unsolicited e-mail originating from Sirius' networks or other Internet/Intranet/Extranet service providers on behalf of or to advertise a service hosted by Sirius or connected via the Sirius network is prohibited.

7.8 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) is prohibited.

8. Minimum Access Requirements

8.1 Only computers and other devices issued by Sirius may be connected to any Sirius network.

8.2 If Sirius employees have access to a Sirius-provided computer or device, it is configured to restrict access at the system level, to install up-to-date malware or anti-virus software, to enable the computer's firewall, and to automatically download and install software updates.

8.3 The above security measures must not be deactivated or circumvented under any circumstances.

8.4 If it is determined that any of the above security measures are not working, the device must be disconnected from the Sirius networks and the IT team informed. The device may only be reconnected with the authorisation of the IT team.

8.5 Sirius employees are not permitted to download and install unauthorised software on a Sirius device without the approval of the IT team.

9. Exceptions

Any exception to the policy must be approved by the InfoSec team in advance.