**..... (company name, registration number, hereinafter referred to as "the Supplier"), undertakes to comply with the following Information Security Policy and the minimum information and cybersecurity requirements:**

## 1. Scope

These Minimum Information and Cybersecurity Requirements of Vičiūnų grupė, UAB (hereinafter referred to as "the Requirements") shall be applicable to the Supplier in the performance of the Contract. These requirements cover the Company's information technology and telecommunication devices and microprocessor-based devices, including, but not limited to, teleinformation collection and transmission devices, automation terminals, control systems (HMI), real-time data controllers, general-purpose controllers, teleinformation collection and transmission systems, commercial data controllers, information technology systems, etc. (hereinafter referred to as "the Equipment"), as well as services related to the Equipment.

## 2. Definitions

2.1. "Necessary for work" means that access is granted only to the minimum scope of the information system (infrastructure) or part thereof necessary for the relevant activity or services.

## 3. Compliance Requirements

3.1. Depending on the type of access to the information system (infrastructure), additional technical and organisational requirements specified in the Law on Cybersecurity of the Republic of Lithuania and in the Description of Organisational and Technical Cybersecurity Requirements Applicable to Cybersecurity Entities, approved by the Resolution of the Government of the Republic of Lithuania No. 818 of 13/08/2018 (current version) may be applicable.

## 4. Security Requirements for Teleworking

4.1. After assessing the potential risks and enabling the Supplier to work remotely from a computerised workstation owned by the Supplier, as well as providing remote access to information resources within the Company’s information systems (infrastructure), the Supplier is required to:

4.1.1. use a secure VPN (Virtual Private Network) connection;

4.1.2. make sure that the information systems, computer equipment, and data networks used for remote access are secure and reliable (with up-to-date operating systems and

other software, installed antivirus software, enabled and properly configured firewalls, etc.);

4.1.3. ensure timely and regular monitoring of access rights;

4.1.4. monitor and control activities on an ongoing basis;

4.1.5. ensure the protection of the Company's sensitive information by technical means;

4.1.6. ensure that the remote connection is controlled and aligned with the mutually agreed objectives;

4.1.7. ensure that remote connection and the granting of remote access are carried out in accordance with the "Necessary for work" principle and have an agreed validity period.

**5. General Cybersecurity Requirements**

5.1. The Supplier shall ensure that the Company's approval for the use of any technology implemented or being implemented in the Company has been obtained and that the security of such technology is adequate.

5.2. Users or administrators of Suppliers' information systems (infrastructure) must authenticate themselves using a password or another authentication method.

5.3. When temporary passwords are given to users or administrators of information systems (infrastructure), they shall be unique for each user or administrator and shall be transmitted in a secure manner.

5.4. Passwords cannot be stored or transmitted in clear text. A temporary password may be transmitted in clear text, but separately from the user's or administrator's name, and only if the user or administrator has no means of decrypting the encrypted password received, or if it is not technically feasible for the user or administrator to transmit the password through an encrypted channel or a secure electronic communications network.

5.5. Before being put into operation any information system (infrastructure), administrators of the Supplier's information systems must change the default (manufacturer) passwords to passwords that comply with these Requirements.

5.6. The functions of the information system (infrastructure) administrator must be performed using a dedicated user name, which may not be used for day-to-day information system (infrastructure) user functions.

5.7. The granting of any privileged (e.g., administrator, root) rights to users of information systems (infrastructure) shall be prohibited.

5.8. Each user or administrator of information systems (infrastructure) must be uniquely identifiable.

5.9 All unnecessary factory user accounts (including guest accounts) in the information systems (infrastructure) must be disabled.

5.10. In publicly accessible computerised workstations, the last user's username must not be visible during login.

5.11. Access for the Supplier's personnel must be granted in accordance with the "Necessary for work" principle.

5.12. Remote access to the information systems (infrastructure) using the administrator's account shall be prohibited.

5.13. When accessing information systems (infrastructure) remotely, the user must authenticate his/her identity by means of a password or another authentication method.

5.14. Any unapproved remote access to the Company's information systems/infrastructure, data or equipment shall be prohibited.

**6. Obligations of Third (External) Parties**

6.1. The Supplier undertakes:

6.1.1. to comply with the Company's confidentiality requirements, these Requirements and the processes in place when working with information resources (computers, mobile devices, information media, documents, data and information) issued by the Company;

6.1.2. to protect Personal Data being processed and/or sensitive information and not to disclose them to any other persons or recipients without the Company's prior written consent;

6.1.3. to be liable for any actions by the Supplier's representatives that cause harm to the Company's information systems (infrastructure) and to indemnify the Company for any resulting losses;

6.1.4. to ensure the confidentiality and integrity of the Company's electronic information, and not to disrupt the availability of electronic information through his/her/its actions;

6.1.5. to use only such access rights to the information system (infrastructure) (create, edit, add, or delete) as have been granted;

6.1.6. upon completion of work or when a user leaves his/her workstation, measures must be taken to prevent unauthorised persons from accessing information processed in the information system (infrastructure), such as logging off from the information system (infrastructure), enabling a password-protected screensaver, and similar;

6.1.7. to use only those functions of the information system/infrastructure and the amount of information to which access has been granted;

6.1.8. in the event of an information and cybersecurity incident potentially related to the Company's data or information resources, to inform the Company thereof without delay (but in any case no later than within 24 hours from the time of becoming aware of the incident) orally by phone: +370 670 59912 and in writing by e-mail: soc@vici.eu providing all available information and data related to the incident;

6.1.9. take sufficient measures to manage the risks associated with the third parties the Supplier engages, the work they perform and the supply chain.

6.2. Suppliers shall be prohibited from:

6.2.1. scanning the Company's information systems (infrastructure) for vulnerabilities or otherwise monitoring the data flow of the Company's information systems (infrastructure). If the measures listed in this paragraph are necessary for the provision of direct services, such measures may only be used after prior agreement with the Company's Information Security Officer;

6.2.2. connecting to the Company's information systems (infrastructure) using equipment not provided by the Company (except via the Company's wireless network for Company guests) without the Company's express consent and knowledge;

6.2.3. drinking, eating and smoking in the vicinity of information processing equipment;

6.2.4. arbitrarily changing the network parameters (IP address, etc.) provided;

6.2.5. using programs that may interfere with the operation of the Company's information systems (infrastructure) (scanning, blocking programs, etc.);

6.2.6. independently modifying, repairing, fixing any software or hardware provided by the Company;

6.2.7. using the software and hardware provided by the Company for activities prohibited by the laws of the Republic of Lithuania, for defamatory, offensive, threatening activities or activities contrary to the public morals and morality, for the creation and dissemination of computer viruses, for the sending of malicious information or for any other purpose that may infringe the legitimate interests of the Company or other persons;

6.2.8. installing, storing, using, copying or distributing any illegal software or software that infringes copyright.

**7. Liability**

7.1. If the supervisory authorities specified in the Cybersecurity Law of the Republic of Lithuania identify an information or cybersecurity incident caused by the Supplier's

actions or omissions in the performance of the Contract, and the Company is imposed a pecuniary penalty, the Supplier undertakes, upon the Company's request, to reimburse the Company for the amount of such penalty in accordance with the penalty payment procedure set out in the Contract.

7.2. The Supplier shall be responsible for the proper implementation of the Requirements by any third parties engaged by the Supplier.

**8. Additional Requirements for Software Development**

8.1. The Supplier shall identify, document, and implement initiatives in accordance with generally accepted information security and cybersecurity standards and practices to ensure secure software and hardware development processes. Such initiatives must ensure information security and cybersecurity at all stages of development: training, definition of requirements, design, implementation, validation, release and maintenance.

8.2. The software must not contain user accounts, passwords, or private/confidential

keys that cannot be changed or removed by an authorised end user of the product.

8.3. The software must not contain any user accounts (individual, shared, test environment) that are not documented.

8.4. The Supplier must actively take measures to improve the security quality of the product. Such measures shall comply with generally accepted cybersecurity standards and practices for industrial process management and, where technically feasible, shall include reliability testing, vulnerability management, and software code security testing (including static or binary code analysis).

8.5. When deploying the software being developed or maintained into the production environment, the Supplier shall ensure the hygiene of the code (e.g., it must not contain sample data or scenario code, references to unused libraries, debugging code, or other development tools).

8.6. The development, testing, and production environments of the software being developed or maintained shall be separated.

8.7. End users of the software should not be shown error messages regarding the software code or the server of the software being developed or maintained.

On behalf of the Supplier .....

(name, surname, position, signature, date)

Annex No.1
VG Information security policy
Minimum Information and Cybersecurity Requirements for suppliers