SynoInt

Security policy

Introduction

When we talk about information security, we don't just mean protecting the transmissions between your computer and SynoInt systems and platforms. We do far more to help safeguard your information. At SynoInt, all data subjects' trusts are our top and the most important priority. So, SynoInt has implemented appropriate technical and organisational controls to protect your personal data and information against unauthorised processing and against accidental loss, damage or destruction. Below is information how SynoInt works in the area of security, what security measures have been implemented, what security standards are applicable. However, please be sure you're comfortable with our security measures and this Security policy before using services in SynoInt platforms and systems and accessing your account online.

1.PASSWORDS POLICY

1.1 All passwords are classified as confidential information;

1.2. Passwords must not be transferred or shared with others unless authorized to do so;

1.3. Passwords must be changed if they have been used, obtained or suspected to be obtained by anyone other than the account owner;

1.4. Individual user passwords must not be written down, inserted into e-mail messages or other forms of electronic communications or stored in a file or computer system unless adequately secured;

1.5. Passwords must have at least 8 (eight) characters;

1.6. Passwords must use at least 3 (three) of the 4 (four) available character types: lowercase letters, uppercase letters, numbers, and symbols.

1.7. These requirements are applicable to all passwords of SynoInt`s employees.

1.8. When we ask you to set up a password to access parts of our sites, SynoInt systems and platforms, you must also comply with these requirements for passwords. But the biggest responsibility is for you. You are responsible for choosing a secure password. Especially SynoInt recommends keep password confidential and you should choose a password that you do not use on any other site. You should not share your password with anyone else, including anyone who works for us. Unfortunately, sending information via the internet is not completely secure. Although we will do our best to protect your personal data once with us.

1.9. If you suspect that passwords has been compromised, please inform about this immediately by e-mail info@synoint.com and / or data.protection@synoint.com.

2.NETWORK SECURITY

2.1. SynoInt ensures that network, systems, databases, applications, network components and other computing devices are protected from malicious activity and unauthorised access.

2.2. SynoInt has implemented the appropriate controls such as anti-virus, firewalls, login control and some intrusion prevention systems.

2.3. Anti-virus software and firewalls on all computer devices, servers and networks are updated in accordance with the software providers' recommendations and our network provider ensures that access to sensitive data is limited to properly authorised requests.

3.SERVERS AND BACKUPS

3.1. All SynoInt data and information are stored on encrypted and licensed servers.

3.2. We use third-party servers from Amazon (AWS).

3.3. For data recovery we use automatic database snapshots provided by Amazon.

3.4. We have to inform, that Amazon (AWS) represents, warrants and covenants that according to Amazon (AWS) policies, security is the highest their priority and they comply with all applicable international laws and rules for personal and non-personal data protection and information security. You may also visit https://aws.amazon.com/ and https://aws.amazon.com/compliance/data-privacy-faq/ for details on Amazon (AWS) services and compliance with data privacy.

3.5. For some other data processing (storage) cases, SynoInt uses UAB Interneto vizija services. You may also visit https://klientams.iv.lt/index.php?command=signin and https://sutartys.iv.lt/preview/duomenu_tvarkymas.php for details on UAB Interneto vizija services and compliance with data privacy.

4.PHYSICAL SECURITY

4.1. All the premises of the SynoInt provides the highest level of security.

4.2. The following security features are available on all premises of the SynoInt:

- Premises are locked;
- All premises are with fire extinguishers, smoke and heat detectors;
- All premises are with air conditioning system;
- Monitoring (CCTV), alarm and door access control (ID cards) systems are installed;
- All important documents (in papers) are stored in safes or in lockable cabinets;
- All electronical information is stored in Clouds;
- Also, we have insurances for premises.

5.E-MAIL SECURITY

5.1. SynoInt treats that all e-mails received and sent must be kept confidential and can only be accessed by the persons indicated in the e-mails.

5.2. The e-mails services used by SynoInt meet the data security requirements of the business.

5.3. SynoInt connects to the electronical mailboxes with a secure and recognized SSL / TLS protocol that ensures reliable information encryption. Also, electronical mailboxes are protected against spam.

5.4. All outgoing and incoming e-mails are encrypted, so there is a small possibility that it could be taken over by third parties.

5.5. So, you can safely send e-mails to us and open e-mails where the sender is SynoInt.

6.RELIABILITY OF EMPLOYEES

6.1. Before recruiting, SynoInt investigates that candidates were not be punished in the past for offenses of data protection, information security, confidential and commercial secrets.

6.2. All employees of the SynoInt are of impeccable reputations.

6.3. Also, employees are educated about the information security, working with the software, working with personal data. At least once a year, SynoInt employees are provided special trainings on personal data protection and information security.

6.4. All employees' actions with personal data in SynoInt systems and platforms are reviewed from time to time using the "log files". Also, employees' access to personal and non-personal data is provided through a special system that is called "System access management".

7.HANDLING OF SECURITY BREACHES

7.1. SynoInt is responsible for the confidentiality and security from the moment the personal data is received. Despite best efforts, we cannot always guarantee absolute security because many aspects also depend on you.

7.2. In case a threat has been determined or justifiable suspicions arise for your personal data, SynoInt informs you about such event.

7.3. SynoInt reserves the right to inform and notify law enforcement authorities about security breaches.

7.4. However, you should note that SynoInt did not have any security breach.

8.BUSINESS CONTINUITY AND RECOVERY PLAN

8.1. Despite all the efforts that organizations and companies devote to identifying and addressing external and internal problems related to security, protection of personal data, business continuity, they are constantly faced with unexpected emerging various threats and incidents. The smallest threat / incident can pose a risk for the organization's and company`s operations, threatens its reputation, can ruin management structures, cause significant financial difficulties, or even compromise the company's survival.

8.2. In view of this, SynoInt has prepared Business continuity and recovery plan.

8.3. SynoInt activities may be suspended, terminated, but only temporarily. Following Business continuity and recovery plan, SynoInt can return quickly and continue to operate. The main purpose of the Business continuity and recovery plan is to ensure uninterrupted activity of the SynoInt and identify actions and responsibilities in order to protect against threats and if threats occurred, how to eliminate the consequences of threats.

9. CHIEF INFORMATION SECURITY OFFICER (CISO)

9.1. We would like to inform that in adherence to the best practises on information security, SynoInt has been assigned the following Chief information security officer (CISO):

- Chief technology officer (CTO) Albertas Jurgelevičius (on IT side).

9.2. If you would like to contact SynoInt CISO, you have questions related to the information security or other matters related to information security, please contact by e-mail data.protection@synoint.com and in part "Subject" indicate "CISO".

10. COMPLIANCE WITH ISO

10.1. Information security includes three main aspects:

- confidentiality of information – protection of information against unauthorized disclosure;
- integrity of the information – protection of information from unauthorized or accidental change;
- availability of information – ensuring that information is available whenever it is needed.

10.2. In order to ensure the confidentiality, integrity and availability of information processed by the SynoInt, SynoInt is in process creating information security management system.

10.3. SynoInt intends to open information security management system in first part of 2019 and start certifying according to ISO 27001 (LST ISO/IEC 27001:2013) until at the end of first part of 2019.

11. APPLICABLE LAW AND CHANGES

11.1. This Security policy is governed by the law of the Republic of Lithuania.

11.2. Any dispute, controversy, disagreement or claim arising out of or in connection with the Privacy policy, as well as issues of the violation, termination or validity / invalidity hereof shall be settled by mutual negotiations.

11.3. The main and always updated version of this Security policy is posted in English on www.synoint.com/legal.

11.4. This Security policy might be used by the following sites: www.synoscore.com, www.synoanswers.com, www.synopanel.com, www.synorewards.com , www.s urveyo24.com, www.synokorea.com, www.synojapan.com.