DATA STORAGE AND ACCESS SECURITY REGULATIONS

REV. 2.0

30 June 2021

Rev.:	Owner:	Date:	Changes:
1.0	Jarosław Lubiak/Marta Czarnecka	25/05/2017	Document creation
2.0	Marta Czarnecka-Grzyb	29/06/2021	Update
2.1	Mikołaj Janeczek	30/03/2026	Update

TABLE OF CONTENTS

I. Use of Xelto customers' Confidential Information

1. Every staff member is obliged to keep in strictest confidentiality any and all information received from Xelto customers, including information containing any personal details, data of technical, operating, administrative, economic and legal, corporate, marketing, planning, business, or financial character; information on business strategies, intentions and achievements, terms and conditions of contracts concluded by the Customers, or information concerning any and all devices, prices, technologies, software and business practices used by the Customers.

2. The above obligation refers to all Confidential Information received in connection with the performed tasks, including those assigned directly by Xelto customers or through persons acting on their behalf, be it orally, in writing, electronically, or in any other form, regardless of the type of Confidential Data carrier.

3. The confidentiality obligation does not extend to Confidential Information which: • must be disclosed by operation of law;
   - is disclosed pursuant to a request by an entity authorised to access such Confidential Information, provided that the entity has been informed about the confidential character of the information concerned;
   - is publicly available or has been disclosed to the public by the authorised Party or with its written permission.

4. Should a member of Xelto staff be made to disclose Confidential Information by an order of the Court or a state authority, or such disclosure be necessary by operation of law, they shall inform Xelto management to that effect forthwith.

5. Every staff member undertakes to make every effort to guarantee that the means of communication used by them to receive, transmit, store and use Confidential Information are safeguarded against unauthorised third-party access.

II. Protection of data on portable computers and PC stations

In order to ensure security and confidentiality of the data stored on computer drives, and to protect it against unauthorised access in case or theft or loss, it is mandatory that the drives of computers using the Windows operating systems are encrypted using the BitLocker feature.

Detailed step-by-step encrypting instructions are available from:

https://drive.google.com/file/d/1ptiQxV-cDrpc7o2sL1qMu73b0afVzfg_/view?usp=sharing

III. Protection of data on mobile devices

In order to ensure security and confidentiality of data, and to protect it against unauthorised access in case or theft or loss, it is also mandatory to encrypt mobile phones.

Detailed encrypting instructions are available under the links provided below, depending on the phone operating system:

1. Mobile Android devices

https://drive.google.com/drive/u/0/folders/179YTk8vY1yn-7iHcPWhGd7Pu25PuU7xA

2. Mobile iOS devices

https://drive.google.com/drive/u/0/folders/179YTk8vY1yn-7iHcPWhGd7Pu25PuU7xA

IV. Data backup

In order to improve the storage security of materials related to XELTO's business, it is mandatory to make backup copies on the GDrive. It will enable quick access to the data stored there from any location after logging onto the service account.

Detailed instructions for installation are available from:

https://drive.google.com/drive/u/0/folders/179YTk8vY1yn-7iHcPWhGd7Pu25PuU7xA

V. Antivirus software

Every staff member shall install antivirus software on their computers and update it regularly, following the manufacturer's recommendations.

VI. Rules for using @xelto.com e-mail

Every staff member shall use their company e-mail address and related tools, such as Hangouts, Calendar, Gdrive, etc., for XELTO purposes only.

Every user shall be obliged to leave all messages on the Xelto server.

Every user shall be responsible for the content of their correspondence. Further, they are obliged to follow the internal e-mail use regulations, the Polish law, good practice and customarily accepted rules of etiquette.

Sending SPAM messages and unlawful content shall be prohibited and deemed contrary to these Regulations.

All e-mail shall be XELTO's property. The Xelto domain administrator shall be authorised to access the content of the messages in emergency situations, i.e. if required to protect Xelto's interests and security, of the interests and security of its Customers and staff.

Every e-mail user shall keep their password secret and not disclose it to third persons.

Thank you in advance for your cooperation in quickly implementing these

Regulations!