Information Security Policy

Custom Group

20.09.2024

Custom Medical &
Custom Interactions Germany
Robert-Bosch-Strasse 7
64293 Darmstadt

Custom Medical US
One Boston Place – Suite 2600
Boston MA 02108, USA

www.custom-medical.com
www.custom-interactions.com

Document Review

	Date	Role & function	Name	Signature
Author	20.09.2024	ISO	Benjamin Franz	B. Franz
Review & Approval	20.09.2024	CEO	Michaela Kauer-Franz	Michaela Kauer-Franz

Revision History

Rev.	Date	Description of change & reason
D	20.09.2024	▪ Added a way to contact ISO from outside of the company ▪ Adjustment of some chapters to be more specific on stakeholders from the outside of the company
C	30.07.2024	▪ Changed Information Security Coordinator to Information Security Officer (ISO) and added responsibilities needed for ISO 27001 ▪ Signature-field deleted at the end of document and referred to cover page ▪ Extension of various chapters to also include management of Personally Identifiable Information (PII); updated responsibility of ISO and general definition of PII; Addition of some paragraphs on PII in chapter 4.7 Data Protection ▪ Chapter 4.11 Clear Desk and Clear Screen added ▪ Added explicit mentioning of IS requirements and continous improvement of the ISMS to chapter 4.1 ▪ Added chapter on secure disposal or re-use of equipment (chapter 4.12) ▪ Information Transfer rules defined in chapter 4.13 ▪ Added quality manager as another defined responsibility in chapter 4.3
B	10.06.2024	Section for Document Review and Revision History added Corrected text on number of confidentiality levels (former “two” was incorrect)
A	08.03.2024	Initial creation

Table of Content

1 Preamble

This Information Security Policy establishes the principles, guidelines, and responsibilities for protecting the information assets of all members of the Custom Group in accordance with the ISO 27001 standard. This policy outlines the commitment of the Custom Group to maintain the confidentiality, integrity, and availability of information and to comply with legal, regulatory, and contractual requirements related to information security.

2 Policy Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to Custom Group's information assets, including but not limited to:

- Electronic data
- Physical documents & facilities
- Communication channels & networks
- Software applications
- Hardware devices

For all clients requiring TISAX certification, the annex I TISAX also applies.

3 Information Security Objectives

The primary objectives of this policy are to:

- Protect the confidentiality of sensitive information belonging to the Custom Group and its clients.
- Ensure the integrity and accuracy of data and information.
- Maintain the availability of information systems and resources.
- Comply with applicable legal, regulatory, and contractual requirements related to information security.
- Promote a culture of awareness and accountability regarding information security among employees and stakeholders.
- Manage Personally Identifiable Information (PII) and to ensure it is collected, used, stored, and disclosed in a manner that complies with applicable privacy laws and regulations, including GDPR.

4 Information Security Responsibilities

4.1 Management Commitment

The Custom Group's management is responsible for establishing, implementing, and maintaining an Information Security Management System (ISMS) based on ISO 27001 standards by satisfying applicable requirements, ensuring adequate resources are allocated, promoting a culture of security awareness and compliance as well as continuously improving the ISMS based on current developments and regulations.

4.2 Information Security Officer

The Information Security Officer is entitled by the management to be responsible for overseeing the implementation and enforcement of information security policies, procedures, and controls of the ISMS. This includes the responsibility to ensure that the ISMS conforms to the requirements of ISO 27001 and to report on the performance of the ISMS to the management (i.e., once a year during management review).

The ISO is further responsible for the overseeing the management and especially the protection of Personally Identifiable Information (PII). He is supported by an external Data Protection Officer (DPO).

To reach the ISO use this email: iso@custom-interactions.com or from within the company the CAPA-System.

4.3 Quality Management Officer

The quality manager supports the ISO in the area of internal and external audits as well as the planning and tracking of measures based on IS incidents and suggestions for improvement.

This guarantees that a synergy is created between the QMS and ISMS and that potential problems due to mutual dependencies are identified and eliminated at an early stage.

4.4 Employees

All employees are responsible for understanding and adhering to information security policies, reporting security incidents promptly, participating in security awareness training, and contributing to the effectiveness of the ISMS.

4.5 Access Control

Access to the Custom Group's information assets shall be granted based on the principle of least privilege and need-to-know. To ensure this, during the role-onboarding process rights are granted based on the role of the employee. Rights are revoked / changed during role changes / offboarding.

Employees must use unique login credentials and passwords for accessing company systems and applications, following the guidelines set forth in the ISO 27001 standard. Access to sensitive information must be protected through encryption, and other appropriate security measures in accordance with ISO 27001 requirements. If customers require special access control to their specific information, this will be coordinated individually.

Data provided by customers requesting TISAX certification will be handled according to the TISAX annex of the information security policy.

Access to and from suppliers to data is handled according to the Annex “Suppliers” of this information security policy.

4.6 Information Classification

All information assets shall be classified based on their sensitivity and importance to the Custom Group and its clients. The Custom Group defines three levels of information confidentiality:

- Confidential: Information that, if disclosed, could cause significant harm to Custom Group, its clients, or stakeholders.
- Internal use: Information intended for internal use only, not to be disclosed outside of Custom Group.
- Public: Information intended for public release and does not require protection.

As general rule, the Custom Group classifies all information in projects as confidential, if not otherwise approved by the management team. All other information is classified as internal if not otherwise approved by the management team. Any information that is intended to be made public is automatically classified as public upon release (e.g., marketing materials). Appropriate controls shall be applied based on the classification level.

4.7 Data Protection

Personal and sensitive information shall be protected against unauthorized access, disclosure, alteration, or destruction. Encryption and other security measures shall be employed to safeguard data in transit and at rest. Regular backups must be performed to ensure data availability in the event of system failure or data loss.

Protection especially concerns the handling of Personally Identifiable Information (PII), which includes any information that can be used to identify an individual, either directly or indirectly, including but not limited to names, addresses, phone numbers, email addresses, identification numbers, and financial information. PII shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures and shall further be restricted to authorized personnel only. PII always classifies as confidential information. Data subjects are informed about their rights and can exercise their rights under applicable privacy laws, including the rights to access, rectify, erase, and restrict the processing of their PII.

As an additional measure, PII from test participants are pseudonymized for employees and made available anonymously to clients for evaluation.

If relevant, specific Data Processing Agreements are signed to ensure that third-party data processors include GDPR-compliant data processing agreements, outlining the processor's obligations regarding PII protection.

4.8 Network Security

Network infrastructure shall be protected against unauthorized access, intrusion, and malicious activities through the implementation of firewalls, intrusion detection/prevention systems, and regular security assessments. Intrusion detection systems need to be implemented to protect data from outside access. To ensure network security the access from computers not belonging to the Custom Group needs to be restricted.

4.9 Physical Security

Physical access to facilities, equipment, and storage areas containing sensitive information shall be restricted to authorized personnel only. Access to these areas is depending on the role of the employee. If people outside of the Custom Group gain access to the networks and servers of the company, they must be secured in a way that prevents data access as far as reasonable possible.

4.10 Incident Response

An incident response plan shall be developed and maintained to effectively respond to security incidents, breaches, or unauthorized activities. Any suspected or confirmed security incidents shall be reported to the Information Security Officer and IT department. You can do so by writing an email (see chapter ISO). From within the company please use the CAPA-system with the option "information security incident".

4.11 Clear Desk and Clear Screen

All personnel must ensure that sensitive information, whether in electronic or physical form, is protected from unauthorized access and visibility. This is achieved through the practice of keeping workspaces clear of unprotected sensitive information and locking computer screens when not in use.

Accordingly, the following points must be complied with:

Clear Desk Procedures

- End of Day Routine: All employees must clear their desks at the end of each workday. This includes securing all documents, notes, and storage media (e.g., USB drives, CDs) containing sensitive information in locked drawers or cabinets or need to be marked as "confidential".
- Temporary Absence: When leaving the desk for a short period (e.g., lunch break, meeting), employees must ensure that sensitive documents are not left visible. Documents should be placed in drawers or covered.
- Confidential Waste Disposal: All sensitive documents that are no longer needed must be disposed of in designated confidential waste bins or shredders.

Clear Screen Procedures

- Manual Screen Lock: Employees must manually lock their computer screens (e.g., by pressing Win+L) whenever they leave their desk.
- Visible Information: Employees must ensure that sensitive information on computer screens is not visible to unauthorized persons, especially in public or shared areas. Privacy screens should be used if necessary.

Physical Security

- Secure Storage: Use lockable storage for sensitive information. Access to these storage areas should be restricted to authorized personnel only.
- Visitor Management: Ensure that visitors are escorted in areas where sensitive information is processed or stored, and that they do not have unsupervised access to such information.

Mobile and Remote Work

- Remote & Off-Premises Workspaces: Employees working remotely or off-premises must ensure that their workspace adheres to the same clear desk and clear screen principles.
- Transporting Information: When transporting sensitive information, ensure it is securely stored and not left unattended.

4.12 Secure Disposal or Re-Use of Equipment

The organization is committed to securely managing the disposal or re-use of equipment to protect sensitive information from unauthorized access and to comply with relevant legal, regulatory, and contractual requirements.

Accordingly, the following points must be complied with:

- Data Wiping: Ensure that all data is securely erased from equipment before disposal or re-use.

- Internal Re-Use: Before re-using equipment within the organization, ensure that all previous data is securely erased and the equipment is reconfigured for its new purpose.
- External Re-Use: When transferring equipment to external parties (e.g., donations, resale), ensure all data is securely wiped.

4.13 Information Transfer Rules

To ensure the protection of information transferred within the organization and with external entities, maintaining its confidentiality, integrity, and availability.

1. Identification and Classification of Information
   - **Classification:** These rules specifically apply for the transfer of confidential information, as public information can be shared freely and internal use information is not to be shared with third parties anyway.
2. Secure Electronic Communications
   - **Encryption:** Sensitive information transferred electronically should be encrypted (e.g. by using encrypted harddrives or the file transfer option).
   - **File Transfers:** Use secure file transfer methods (e.g., SFTP, FTPS, HTTPS) for sharing files containing sensitive information (e.g. password protected and timely limeted access to specific folder on server)
3. Physical Transfer of Information
   - **Physical Documents:** Sensitive documents must be transported in sealed, tamper-evident packaging and should be hand-delivered or sent via secure courier services.
   - **Access Control:** Limit access to physical documents to authorized personnel only.
4. Third-Party Transfers
   - **Third-Party Agreements:** Ensure that third-party service providers and partners comply with the organization’s information transfer policies and procedures (sign dedicated NDA or DPA to control data exchange).
   - **Confidentiality Agreements:** Require third parties to sign confidentiality agreements before sharing sensitive information (see above).
   - **Verification:** Verify the identity and authorization of third parties before transferring sensitive information.

5 Compliance and Monitoring

5.1 Compliance

Compliance with this Information Security Policy shall be periodically reviewed, assessed, and audited to ensure adherence to established security standards and requirements. This is done together with the yearly internal audits of our quality management system. The results of the internal audits are documented in an audit report and presented in the yearly management review to ensure that the Custom Group’s management team has a chance to review the effectiveness and efficiency of the information security management system.

5.2 Monitoring

Information security controls, systems, and activities shall be monitored regularly to detect and mitigate potential security risks and vulnerabilities.

6 Training and Awareness

6.1 Training

All employees shall receive appropriate training and education on information security policies, procedures, and best practices relevant to their roles and responsibilities in safeguarding company information. This training is part of the onboarding training. Due to its immense importance the training is repeated by every employee on a yearly basis together with the data protection training and the partaking needs to be countersigned by each employee.

6.2 Awareness

Regular communication and awareness programs shall be conducted to promote a culture of security awareness and accountability among employees.

This is done by using the company wide "tools and technical support"-channel as well as during daily & weekly team meetings.

7 Policy Review and Update

This Information Security Policy shall be reviewed and updated periodically to reflect changes in the business environment, technology landscape, and regulatory requirements. This is done at least once a year during the management review as response to the internal audit and incident reports.

8 Policy Acknowledgement

All employees working with confidential or internal information shall be required to acknowledge their understanding and acceptance of this Information Security Policy. The same applies to any contractors, vendors, and third parties outside the company that handle confidential information and are considered medium or higher risk.

9 Policy Enforcement

Failure to comply with this Information Security Policy may result in disciplinary action, termination of employment / contracts, or legal consequences as deemed appropriate by the Custom Group's management.

All violations of this policy must be immediately reported to the ISO via email or from within the company via the CAPA-System. In case of intentional or grossly negligent violation of this policy the Custom Group reserves the right to terminate the employment contract / other contract without notice.

10 Policy Communication

This Information Security Policy shall be communicated to all relevant stakeholders, including employees, contractors, vendors, and third parties, through appropriate channels. Those channels are:

- From outside the company: Companys website
- From within the company:
  - QM Server
  - Relevant updates will be published also in the “announcement channel”.

11 Policy Documentation

This Information Security Policy shall be documented, maintained, and made available through all channels mentioned in chapter “Policy Communication”.

12 Contact Information and Policy Approval

For questions or concerns regarding this Information Security Policy, please contact the designated Information Security Officer (see chapter ISO) or the IT department from within the company.

By adhering to this Information Security Policy, we can ensure the confidentiality, integrity, and availability of our information assets and maintain the trust of our clients and partners.

This Information Security Policy has been approved by the Custom Group's management and shall be effective in the current version as of the date of approval (see cover page).