EMEA
TECHNICAL AND ORGANISATIONAL MEASURES
(TOMs)

Version Change/Review History

Release/ Version	Date	Author(s)	Revision Details
1.0	25.05.2018	Gerhard Smischek	Original Document
2.0	01.02.2021	Mateusz Leszczynski	Moved to new template format. Moved Versioning to common nomenclature. Moved to the concept of ISO/IEC 27001:2013 and Exela ISO 27001 certification program. EMEA-wide extended.
2.1	19.05.2021	Bernhard Hofmann	Language corrections for the German version
2.2	20.05.2021	Oleg Simanic	Release
3.0	21.07.2021	Mateusz Leszczynski	Territorial scope update: removed 2 closed premises, added 1 newly certified premise; Release

Preamble

Exela Technologies (hereinafter referred to as 'Exela') is a business process automation (BPA) leader, leveraging a global footprint and proprietary technology to provide digital transformation solutions enhancing quality, productivity, and end-user experience. The business of Exela, which is under the scope of this document, is design, development, implementation and support of document management & image processing, data capture, workflow solutions, software support services, and managed services including print, mail & despatch.

Exela intends to maintain security of personal data in accordance to the GDPR and UK-GDPR and ensures that Customer's data will be processed in a safe manner. Following document presents appropriate technical and organisational measures whose level of protection adequately corresponds to the risks of Exela's processing activities. Information security management describes controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

The measures which have been taken are those which ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of the GDPR and UK-GDPR have been taken into account. For orientation purposes, reference is made to the concepts of ISO/IEC 27001:2013 "Information security management systems" Annex A.

Territorial scope

Following TOMs are applicable for EMEA region and refers to the ISO/IEC 27001:2013 certified Exela premises listed below:

1. Exela Technologies, Baronsmede House, 20 the Avenue, Egham, TW20 9AB, United Kingdom;
2. Exela Technologies, Sandringham House, Sandringham Avenue, Harlow Business Park, Harlow CM19 5QS, United Kingdom;
3. Exela Technologies, Barclays House, 1 Wimborne Road, Poole BH15 2BB, United Kingdom;
4. Exela Technologies, Moulton House, 10 Pond Wood Close, Moulton Park, Northampton NN3 6DF, United Kingdom;
5. Exela Technologies, 8 Beckett Way, Park West, Nangor Road, Dublin 12, Ireland;
6. Exela Technologies, Vastberga Alle 36A, Hagersten, Stockholm 120 23, Sweden;
7. Exela Technologies, Eskilstunavagen 34, Strangnas 645 34, Sweden;
8. Exela Technologies, Gripengrand 4, Froson 838 80, Sweden;
9. Exela Technologies, Eskilstunavagen 34, Strangnas 645 34, Sweden;
10. Exela Technologies, Nedre Rommen 5C, Oslo 0988, Norway;
11. Exela Technologies, Plauener Str. 163-165, Berlin 13053, Germany;
12. Exela Technologies, Hubnerstrasse 3, Augsburg 86150, Germany;
13. Exela Technologies, Monzastrasse 4c, Langen 63225, Germany;
14. Exela Technologies, Grudziądzka 46-48, Toruń 87-100, Poland;
15. Exela Technologies, 1 Rue de la Mare Blanche, Noisiel 77186, France;
16. Exela Technologies, 14 Rue des Landelles, Cesson Sevigne, Ille-et-Vilaine 35510, France;
17. Exela Technologies, ZAC des Foliouses, Rue de Monts d'Or, Miribel les Echets 01700, France;
18. Exela Technologies, Uraniumweg 15, 3812 RJ Amersfoort, Netherlands
19. Exela Technologies, Monzastrasse 4c, Langen 63225, Germany.

Confidentiality, integrity, availability and resilience of processing systems and services.

I.Physical and environmental security

Relevant ISO-controls: A.11.1.1 Physical security perimeter; A.11.1.2 Physical entry controls; A.11.1.3 Securing offices, rooms and facilities; A.11.1.4 Protecting against external and environmental threats; A.11.1.5 Working in secure areas

Exela has implemented required measures, those are among others:

☒ All relevant doors and/or windows are suitably protected against unauthorized access with control mechanisms (e.g. locks, bars, alarms, badge readers, magnetic cards);

☒ Where required, additional barriers and perimeters to control physical access between areas in same building are in place (e.g. for server rooms);

☒ Access to sites and buildings are restricted to authorized personnel only;

☒ Access rights are being granted on a need-to-know basis and are being regularly reviewed and updated, and revoked when necessary;

☒ The date and time of entry and departure of visitors are being recorded, and all visitors are being supervised by Exela member of staff, unless their access has been previously approved;

☒Photographic, video, audio or other recording equipment, such as cameras in mobile devices are not allowed, unless their use has been previously approved;

☒ Physical protection against natural disasters, malicious attack or accidents are designed and applied in line with national, regional or international standards.

II.Access Controls

Relevant ISO-controls: A.9.1.1 Access control policy; A.9.1.2 Access to networks and network services; A.9.2.2 User access provisioning; A.9.2.4 Management of secret authentication information of users; A.9.4.2 Secure log-on procedures; A.9.4.3 Password management system; A.12.4.1 Event logging; A.12.4.3 Administrator and operator logs;

Exela has implemented required measures, those are among others:

☒ Access control policy is established, document and reviewed on regular basis. It covers among others: segregation of access control roles (e.g. access request), requirements for formal authorization and periodic review of access requests;

☒ Management controls and procedures to protect access to network connections and network services and the means used to access networks and network services (e.g. use of VPN) are in place;

☒ Need-to-know and need-to-use principles are followed;

☒ Process for assigning or revoking access rights granted to user IDs is in place and includes among others: ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed. Furthermore, Exela maintains a central record of access rights granted to a user ID to access information systems and services;

☒ Secret authentication information is controlled through a formal management process;

☒Where required by the access control policy, access to systems and applications shall are controlled by a secure log-on procedure;

☒Password management systems are interactive and ensure quality passwords (e.g. users are forced to change their password on regular intervals and we follow a rule to not display passwords on the screen when being entered).

☒Event logs recording user activities, exceptions, faults and information security events are maintained and regularly reviewed.

III. Asset and data management

Relevant ISO-controls: A.8.1.1 Inventory of assets; A.8.2.1 Classification of information; A.8.2.2 Labelling of information; A.8.3.1 Management of removable media; A.12.2.1 Controls against malware; A.12.3.1 Information backup;

Exela has implemented required measures, those are among others:

☒ Exela identified assets and its owners in the lifecycle of information, documented their importance and created an inventory of these which is maintained on regular basis;

☒ Classifications and associated protective controls for information includes business needs for sharing or restricting information, as well as legal requirements. The level of protection in the scheme are assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered. Owners of information assets are accountable for their classification;

☒ An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted within Exela. Employees are aware of labelling procedures;

☒ Procedures for the management of removable media in accordance with the classification scheme are implemented (e.g. all media are stored in a safe, secure environment, in accordance with manufacturers' specifications);

☒ Detection, prevention and recovery controls to protect against malware are implemented combined with appropriate user awareness;

☒ Backup copies of information, software and system images are being tested regularly in accordance with an agreed backup policy;

☒ The backups are being stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

IV. Communication

Relevant ISO-controls: A.13.1.1 Network controls; A.13.1.3 Segregation in networks; A.13.2.2 Agreements on information transfer; A.13.2.4 Confidentiality or nondisclosure agreements

Exela has implemented required measures, those are among others:

☒Networks are managed and controlled to protect data in systems and applications (e.g. systems connection to the network is restricted and authenticated, special controls are established to safeguard the confidentiality and integrity of data);

☒ Groups of information services, users and information systems are segregated on networks. Access is controlled at the perimeter using a gateway (e.g. firewall);

☒ Transfer agreements are in place;

☒ Non-disclosure agreements reflecting Exela's needs for the protection are identified, regularly reviewed and documented.

V.Compliance

Relevant ISO-controls: A.18.1.1 Identification of applicable legislation and contractual requirements; A.18.1.3 Protection of records; A.18.1.4 Privacy and protection of personally identifiable information

Exela has implemented required measures, those are among others:

☒ All relevant legislative statutory, regulatory, contractual requirements are identified, documented and kept up to date. The specific controls and individual responsibilities to meet above are also defined and documented;

☒ All data is being protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements;

☒Privacy and protection of personal data is ensured as required in relevant legislation and regulation where applicable, especially including GDPR and UK-GDPR.

The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

I. Incident management

Relevant ISO-controls: A.16.1.2 Reporting information security events; A.16.1.3 Reporting information security weaknesses; A.16.1.4 Assessment of and decision on information security events; A.16.1.5 Response to information security incidents; A.16.1.7 Collection of evidence

Exela has implemented required measures, those are among others:

☒ Relevant procedures and processes to ensure a quick, effective and orderly response to information security incidents are implemented and regularly reviewed. Classification and prioritization of incidents is defined;
☒ All employees are aware of their responsibility to report information security incidents as well existence of procedures for reporting and the point of contact to which the events shall be reported;

☒ Collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices are defined.

II. Continuity management

Relevant ISO-controls: A.12.3.1 Information backup; A.17.1.1 Planning information security continuity; A.17.1.2 Implementing information security continuity; A.17.2.1 Availability of information processing facilities.

Exela has implemented required measures, those are among others:

☒ Requirements for information security and the continuity of information security management in adverse situations (e.g. during a crisis or disaster) have been defined;

☒ Processes, procedures and controls are established, documented, implemented and being maintained to ensure the required level of continuity for information security during an adverse situation;

☒ Information security management continuity is being verified by among others exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;

☒ Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended;

☒ Backup media are regularly tested to ensure that they can be relied upon for emergency use when necessary.

Assessing and evaluating the effectiveness of technical and organisational measures

I. Reviews

Relevant ISO-controls: A.18.2.1 Independent review of information security; A.18.2.2 Compliance with security policies and standards; A.18.2.3 Technical compliance review

Exela has implemented required measures, those are among others:

☒ Controls, objectives, policies, processes and procedures are being reviewed independently at planned intervals and/or when significant changes occur.

☒ We conduct an additional actions in case of any non-compliance is found (e.g. identify the causes of the non-compliance; evaluate the need for actions to achieve compliance; implement appropriate corrective action; review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses);

☒Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented.

Pseudonymisation and encryption of personal data

Relevant ISO-controls:

A.10.1.1 Policy on the use of cryptographic controls; A.10.1.2 Key management; A.14.3.1 Protection of test data; A.18.1.5 Regulation of cryptographic controls

Exela has implemented required measures, those are among others:

☒ Policy on the use of cryptographic controls for protection of information is developed and implemented;

☒ Based on a risk assessment, the required level of protection is identified taking into account the type, strength and quality of the encryption algorithm required;

☒ Policy on the use, protection and lifetime of cryptographic keys is developed and implemented. Cryptographic algorithms, key lengths and usage practices should are being selected according to best practice;

☒ All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys are physically protected;

☒ Any test data is being selected carefully, protected and controlled;

☒ Cryptographic controls are in compliance with all relevant agreements, legislation and regulations.