**CXS Connected Enterprise and General Data Protection Regulation**

**Background**

The deployment of effective, relevant information security and data protection controls is fundamental to CXS Connected Enterprise’s market proposition as a leading provider of Data Centre, Connectivity, Cloud and Managed Services. CXS Connected Enterprise is committed to securing and protecting the personal data in its custody.

The General Data Protection Regulation (GDPR) comes into force on the 25th May 2018, at which point it will supersede the current Data Protection Act 1998 (DPA).

While GDPR is a complex piece of legislation, it is important to remember that it builds upon the requirements defined within the DPA, which already provides a substantial body of law around the security and protection of personal data.

CXS Connected Enterprise already complies with the DPA. CXS Connected Enterprise’s own GDPR programme has been structured to critically assess the existing information security and data protection controls against the more prescriptive requirements of GDPR. Where necessary, the existing controls within CXS Connected Enterprise’s Information Security Management System (ISMS) have been updated, extended.

**What Personal Data is CXS Connected Enterprise collecting and how it is processed?**

As a Data Controller, our collection of personal data is limited to only data necessary for the purpose of supporting an effective business relationship with our resellers and direct customers. Reseller (Customer) name and contact details are collected, together with other business data, such as, business address, business contact and payment details.

As a Data Processor, the collection of personal data, provided by the reseller or authorised user within the end-user’s organisation, is limited to the online user-id of the end-user, for the purpose of facilitating the consumption of the selected CXS Connected Enterprise service.

CXS Connected Enterprise does not collect any special category of personal data.

**CXS Connected Enterprise will only process personal data where:**

processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

or

processing is necessary for compliance with a legal obligation to which CXS Connected Enterprise is subject

or

where the data subject has given consent to the processing of his or her data for one or more specific purposes

The CXS Connected Enterprise Privacy Policy, available on the CXS Connected Enterprise website (https://www.cxs.co.uk/legal/privacy-policy) provides additional information on how CXS Connected Enterprise commits to handle personal data in line with GDPR.

A data mapping exercise has been conducted for both CXS Connected Enterprise’s customer services and internal systems. These, in turn, have fed into a series of Data Privacy Impact Assessments, to identify potential risks to the security and privacy of the personal data. Where necessary, additional controls have been implemented to mitigate any potential risk.

**CXS Connected Enterprise relationship with third parties.**

**Reseller / Customer**

CXS Connected Enterprise’s Reseller Agreement and Customer Agreement documents have been updated to incorporate the required GDPR clauses. These are available to the Reseller and Customer community through the CXS Connected Enterprise Customer or Channel Portal

The Service Specific Terms (SST) which describe each of the services offered by CXS Connected Enterprise are being updated to satisfy the requirements of GDPR. All of the updated SSTs will be available through the Channel and Customer portal before 25th May.

**Direct Line Vendors**

Each vendor has provided, or committed to providing, a revised GDPR contract (or addendum) by 25th May. The revised contractual terms will be reflected in the updated SSTs, thus ensuring the obligations to secure and protect personal data and the need to support the Data Subject in exercising their fundamental rights is contractually recognised across the service delivery supply chain.

**Other suppliers**

CXS Connected Enterprise has also updated its contractual terms, in line with GDPR, with the suppliers and partners that process personal data in support the CXS Connected Enterprise internal business processes. As above, the revised contractual terms ensure the obligations to secure and protect personal data and the need to support the Data Subject in exercising their fundamental rights is recognised by our suppliers.

The CXS Connected Enterprise Privacy Policy (https://www.cxs.co.uk/legal/privacy-policy) provides additional information on which categories of organisations we disclose personal data in support of our internal business processes.

**CXS Connected Enterprise’s technical and organisational controls.**

CXS Connected Enterprise’s IT architectural model is based upon industry standard equipment and operating system software, deployed across multiple geographically separated datacentres throughout Europe. A highly resilient network designed and built in house, provides connectivity to the Internet and between multiple datacenters, allowing services to be delivered from any datacentre at any time.

The deployed network security architecture utilises multiple layers of proximity firewalls, IDS and IPS, DDoS Mitigation, Proxy Servers and a structure of backbone and core routers and switches configured to deliver the required network segmentation to protect the core environment from unauthorised access. Annual network penetration tests are conducted by two independent third parties.

The final element of CXS Connected Enterprise’s Network Upgrade project, installation of new 100G Dark Fibre rings will be completed by September 2018.

The hardware infrastructure supporting the delivery of the CXS Connected Enterprise services is configured with the required level of resilience to meet the committed service availability levels, with a level of redundancy built into the individual hardware components.

All core service server hardware is protected by F-Secure anti-virus. All servers are subject to a regular schedule of vulnerability scans and subject to a formal Patch Management Policy. All servers are visible to, and managed through, a well-established availability and performance monitoring regime. Logging and audit information is captured for critical resources.

Encryption of ‘data at rest’ is based on server hardware, virtualisation and operating system level encryption techniques.

Access by core staff to all CXS Connected Enterprise resources is controlled through multiple layers of authentication based around a 3-challenge point model. All granted access rights are on a ‘least privilege’ basis, in support of a role-based security model.

CXS Connected Enterprise has appointed a DPO, suitably qualified, to independently assess our compliance to GDPR. A Data Privacy training module has been added to our LMS (Learning Management system), with completion monitored. All employees have signed confidentiality agreements and are exposed to on-going training for information security and data privacy throughout the year and all staff are BPSS cleared. Senior service and technical engineers also carry additional checks performed by QinetiQ and Technical Directorship carries SC Clearance.

All Information Security Policy and Procedure documentation within the CXS Connected Enterprise ISMS has been reviewed and updated, as required. CXS Connected Enterprise’s ISMS aligns to the requirements of ISO9001:2015, ISO27001:2013, BPSS and TSC SC. The process to gain formal certification has already commenced.

Project Management within CXS Connected Enterprise has been enhanced to embrace the ‘Privacy by Design and by Default’ philosophy embodied in GDPR.

CXS Connected Enterprise has upgraded its Incident Management System to include the 72-hour breach notification requirement.

**Summary**

As noted earlier, effective information security and data protection controls is fundamental to CXS Connected Enterprise’s market proposition as a leading provider of Cloud Services. CXS Connected Enterprise is committed to securing and protecting the personal data in its custody.

Building on an existing, comprehensive base, the GDPR Programme has further strengthened CXS Connected Enterprise’s information security and data privacy controls.

CXS Connected Enterprise is committed to its obligations under GDPR, both in its role as Data Controller and as a Data Processor.