DSPT information to assist care providers

Company name Nourish Care
Product name Nourish Information Security Management System (ISMS)

DSPT Number	Aproaching standards	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
1.2.1	Yes	Does your organisation have up to date policies in place for data protection and for data and cyber securityConfirm that your organisation has a policy or policies in place to cover: Data Protection, Data Quaility, Record Keeping, Data securityand, where relevant, network security.	Does your data processing agreement impact the care provider, if so please document your policy and the scope where it would affect the customer	Nourish Information Security Management System (ISMS) applies to the entire Nourish business and its functions. This includes information systems and networks, including servers hosted in Amazon Web Services and Microsoft Azure, physical office environment and people supporting these business functions. It includes procedures for data security, protection & quality, record management, and network security. Nourish ISMS has gone through a stringent certification process to ensure that best practices and comprehensive security controls are in place. Nourish ISMS, has been independently audited by BSI and is ISO 27001:2013 certified. By showing ISO 27001:2003 certificate Nourish is compliant with this, and the supplier can confidently confirm compliance with this and other questions in the DSPT
1.4.1	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Please explain how your product manages and shares personal information	Nourish holds a GDPR Information Register and data flow diagrams detailing the processing, reasons to process, and other.
1.6.1	Yes	Does your organisation's data protection policy describe how you keep personal data safe and secure?	Please explain how your product keeps personal data secure	
1.6.4	Yes	What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately? Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question.	Do you manage customers mobile phones, if so please give your emplanation of how this impact your customers.	Devices provided by Nourish are, by default, enhanced with MDM, which gives the Care Provider several controls to reduce risk of data breach, in particular "Device locking and erasing", Screen Auto-Lockout;
1.6.5	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data? This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO	Please provide your DPIA templates	Nourish certified information security management system includes procedures to ensure that any changes are managed, and associated risks are managed and mitigated using a Data Protection Impact Assessment (DPIA).
1.6.6	No	If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	Does your product have any tools to manage BYOD devices? If so please document how this helps a customer	Nourish has an acceptable use policy, that applies to Nourish staff, and it covers BYOD and is available upon request. Devices supplied to clients are protected as per answer in cell E8
1.7.4	Yes	Does your organisation have a timetable which sets out how long you retain records for?	Please document your data retnention criteria	Nourish follows the statutory requirements for Records Management Code of Practice for Health and Social Care
1.8.3		What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	Please give the reverse of the question, explainined what they have implemented to mitigate risks, so the customer can rank them for all systems in use by them	

DSPT information to assist care providers

Company name Nourish Care
Product name Nourish Information Security Management System (ISMS)

DSPT Number	Aproaching standards	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
4.1.2	Yes	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Please document how your product provides access control and audit of this information	Nourish can supply an audit log of accesses to Nourish, detailing user name and time the user logged in to Nourish.
4.2.5	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	If your product can assist in managing access rights then please explain here	Nourish provides a mechanism to remove an end-user access to Nourish. This is done securely by an authorised member of staff. Nourish provides a mechanism to change an end user's role and access permissions
4.5.4	Yes	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice? If your organisation has any It systems or computers it should provide advice for setting and managing passwords. Each person should havve thier .l;own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be "strong" i.e. hard to guess.	If your product can assist in managing password practice then please explain here	Nourish has a policy in place for password management, that includes displaying how strong the password is.
6.1.5	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	Does your product have any tools to give visibility of who has accessed each individual data record?	
6.2.3	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions.	If you provide any of these devices then please explain any malware magement included on them.	Devices supplied by Nourish, are managed through MDM, hence they are kept up to date, and restricted for care use only.
7.1.2	No	Does your organisation have a business continuity plan that covers data and cyber security?	Please explain your business continuity plans for data and cyber security here.	
7.3.1	Yes	How does your organisation make sure that there are working backups of all important data and information? It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them.	Please document your data backup process.	Nourish Platform databases are deployed in multiple availability zones within the UK to provide live replica. They are fully backed up every 24 hours and have continuous incremental back-ups throughout the day.
7.3.4	No	Are backups routinely tested to make sure that data and information can be restored?	Please document your data backup process.	Backups are tested at least every 12 months.
8.3.5	Yes	How does your organisation make sure that the latest software updates are downloaded and installed It is important that your organisation's IT system (s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question.	Does your product have automated updates. If so, please document how this occurs, and how a customer can check which version they are running.	Nourish updates Operating System, databases, software libraries at least once a year, this way it is ensured that the platform is fully supported for longer. Nourish uses AWS patch manager, to effectively manage O/S updates on the server
9.1.1	No	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?	Do you manage any WiFi routers for customers? If so, please explain how.	

DSPT information to assist care providers

Company name Nourish Care
Product name Nourish Information Security Management System (ISMS)

DSPT Number	Aproaching standards	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
9.6.2	No	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people)	Do you store data on customer devices then it is encrypted? If not then how would customers protect local data?	All Data entered into the Nourish Platform is subject to the security measures implemented by Nourish while at rest and in transit. All information transmitted between the Nourish servers and the devices is encrypted (SSL/TLS SHA-256 with RSA encryption). Furthermore, the data is encrypted at rest using AES-256 encryption, which is a strong multi-factor encryption. No data is permanently stored in the devices supplied by Nourish.
10.1.2	No	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Please give contact details here	Nourish holds a GPDR Information Register that details suppliers that process personal data, and a register of contacts details.
10.2.1	Yes	Do your organisation's IT system suppliers have cyber security certification Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace	Please confirm if you have cyber security certification	Nourish is ISO 27001 certified. Certificate is available upon request.
		Has your organisation completed the DSPT?	Have you completed the DSPT , if so where do you display this ?	Yes, This is published on the DSPT portal
		GDPR statement and contract with supplier	Please give a link to your GDPR statement, ideally in as plain English/easy to understand format as possible	As part of Nourish certified Information Security System policies, Nourish has a GPDR statement that is available upon request.