Supply Sector/Solutions Provider V3.1

service delivery module

The voice of technology enabled care

Description

Specific TEC industry standards for service providers have been produced by TSA for over 20 years. More recently, we have seen an increase in demand from commissioners and service providers, for Supply and Solutions Providers to be checked against similar, outcomes focused standards that are specific to the TEC sector.

The QSF allows for Suppliers and Solutions providers to be unique in their offering, but reassures service users, service providers and commissioners, that they are externally validated by industry experts and ensure high levels of quality in service delivery.

Key Outcomes

- **Supply sector organisations will be seen to drive and support the quality and improvement agenda in partnership with services they work with.**
- **The supply sector will be seen as open, honest and approachable, understanding the needs of the sectors in which they work.**
- **That the solutions they provide are resilient and Service User focused.**

The Audit Process will seek evidence that the key outcomes have been met. As a minimum, TEC Quality certified organisations ***must:***

- Have a clear and unambiguous pricing policy, which also indicates the frequency of and how (if any) price increases will be applied.Demonstrate there is an effective product recall/roll-back and customer communication process in place, where suspected design, or reliability faults have been identified.
- Have effective procedures to ensure that suppliers payments are maintained in accordance with agreed terms and conditions, so as not to jeopardise the supply chain
- Conduct risk analysis of their supply chain and shall have implemented actions to mitigate and manage the risk of supply of equipment, or service.
- Have a clear policy, which is included in contractual arrangements and is made known to service providers, on termination of supply of product/services where the safety of Service Users may be affected.
- Have policies and procedures in place to ensure that they work openly with customers and that they are always dealt with fairly and within agreed timeframes.
- Have a process for informing customers of available stock levels and lead times for the supply of equipment, which shall include requirements during any operational difficulties. i.e. Pandemic, Staff shortage, raw material shortages, etc.
- Demonstrate that they achieve contractual requirements for equipment delivery - this should include new and repaired equipment.
- Provide evidence of compliance with all warranties and repairs processes/policies they provide.
- Make information available to customers on target equipment repair times and their performance against those targets. This information shall be made available monthly as a minimum.
- Have written procedures to manage and respond internally to report suspected equipment, system or software design faults.
- This should include but not limited to:
- - Corporate responsibilities
- - Escalation into the complaints process
- - Timescales to resolve
- - Out of hours service
- - How customers/end users are advised or supported through the fault process
- - An analysis and incidents log.
- - Planned corrective action to avoid recurrence.
- Have effective processes for the rollout of security updates, new software upgrades and firmware releases to customers, whilst ensuring that these are kept up to date with operating systems. There must also be processes in place which, demonstrate how systems can be "rolled back" to the last stable versions, in the event of software issues becoming known, or updates and upgrades failing.
- Have a clearly defined product recall and returns policy. This will include:
- - General product returns for repair/replacement of product
- - Product recalls where suspected design, or reliability faults have been identified
- - Customer notification and communication process
- Identify to the customer, any incompatibilities with any systems, products, operating systems or software, where they are not backwardly compatible.

Supply Sector/Solutions Provider V3.1

service delivery module

- Identify to the customer, any incompatibilities with any systems, products, operating systems or software, where they are not backwardly compatible.
- Clearly indicate where equipment, systems, or software is sourced and any sub-contractual relationships for provision.
- Demonstrate that the relevant compliance is obtained when product nomenclature is used, that requires compliance to a British or European Standard.
- Note 1: For example, A product referred to as a "Social Alarm" shall require compliance with BS EN 50134 & BS EN 50136 series of Standards, radio frequency and EMC standards. This would also include compatibility with any quoted alarm communication protocols.
- Note 2. The term "Product" can include software, Information Technology systems, and physical equipment, depending on the type of Solution Provider being audited.
- Have a defined warranty and returns policy where "White Labelling" of equipment is provided on a B2B basis.
- Have procedures and processes in place for the redistribution of equipment for future use and disposal and recycling of equipment that is no longer serviceable. This shall include the cleansing of any Service User-specific data, or settings and the provision of WEEE certificates for equipment disposal.
- Ensure that where they are contracted to conduct maintenance and testing of equipment, that this is completed in accordance with an agreed testing and maintenance schedule
- Demonstrate where they provide technology, such as devices, communications methods, software and/or a platform as part of their scope of supply, that:
- • These are capable of reporting on annualised downtime and single incident downtime on a rolling 12 month basis as a minimum.
- • That guidance is made available to the service provider's Design Authority on how the products should be combined and configured to ensure the service meets the relevant availability, security and performance standards
- Demonstrate that where analogue alarm units are known to be still in service on the next generation telephone networks, that these have been successfully tested against the TSA Analogue to Digital testing specification and the results are openly published to the sector. Suppliers shall work with service providers to monitor failure rates with analogue equipment and support a replacement programme.
- Have processes in place which, where technically possible, enables equipment to be made interoperable between manufacturers equipment and receiving platforms, thus increasing flexibility of use for service providers and service users.
- Ensure that digital alarms that communicate using an IP Protocol, TS 50134 - 9 is used as the primary communication protocol. Alarms that use proprietary protocols, must not be locked down to these proprietary protocols and must have the facility to switch to the European protocol automatically if migrated to another platform that cannot communicate with the proprietary protocol.
- Ensure that only "hybrid" social alarms that communicate in both analogue and digital, or purely digital protocols shall be supplied. It is reccomended that all Social Alarms have the ability to have dual communictation connectivity. Note: The TSA 'Commissioner/Buyer Guidance: Transitioning your Social Alarms Systems from Analogue to Digital' provides detailed guidance.
- Provide Device Management Platform training to TEC Service Provider customers, to ensure the correct programming of devices and frequency of heartbeat and alert notification are in place in accordance with the equipment installation plan.
- Ensure that TEC Platforms have the functionality to provide bespoke customer reports, which are aligned with the QSF requirements. The process to obtain such reports will be documented and customers will have received training in the process
- Platform Providers to import/export data in line with customer contracts but as a minimum via CSV file for each contract showing all core data fields.
- Demonstrate that where they provide technology as a service (hosting, SaaS, IaaS etc) that, the availability of their service is monitored, and reports are produced on a rolling 12-month basis and analysed to ensure resilience standards are complied with.
- The reports shall include but not be limited to:
- • Annualised downtime
- • Single incident downtime.
- Demonstrate that where applicable, their service or product, considers any ethical issues: for example, where surveillance technologies are used (GPS tracking devices etc.).
- Demonstrate that the testing and/or piloting of new equipment for the reliability and connectivity of Devices and an analysis of the communication method is undertaken.
- Provide evidence that existing Class 1 and Class 2 medical devices have followed the process to be MHRA certificated. That renewal of certification is embedded into current processes.
- Provide evidence of the ongoing process/journey to obtaining MHRA certification for new devices that are in development.

Measures of Excellence

- Note: Currently, there are no specific Measures of Excellence, other than the compliance requirements listed above.
- Equipment providers shall make information available on the time to repair equipment.
- Where Suppliers provide technology, such as devices, communications methods, software and/or a platform as part of their scope of supply to a customer then the Supplier needs to demonstrate that: The products are capable of reporting on annualised downtime and single incident downtime. That guidance is made available to the service provider's Design Authority on how the products should be combined and configured to ensure the service meets the relevant availability, security and performance standards.
- Where Suppliers provide technology as a service (hosting, SaaS, IaaS etc), then the Supplier needs to demonstrate that the availability of their service is monitored, and reports are produced and analysed to ensure resilience standards are complied with. The reports should include but not be limited to: Annualised downtime, Single incident downtime.

Note: Organisations must also comply with the Performance and Contract Monitoring module requirement for evaluation of performance.

Evidence might include:

- Ethical Marketing Policy
- Anti Bribery Policy
- Anti Corruption Policy
- Complaints/Compliments Policy

- Customer Contracts
- Data Sharing Agreements
- Partnership Working Policy
- Stock Keeping Records/System Reports

- Contract Meeting Minutes
- Service User Feedback Surveys
- Measures of Excellence Reports