17/02/1180 Customer Services Team Service Desk

Specification

Must Haves

ID	Category	Requirement Statement
FR -001	Enquiry/case management	The system will allow users to create a customer record
FR -002	Enquiry/case management	The system will allow users to record all customer queries received by e-mail, over the phone, in post, through despatch box and in person
FR -003	Enquiry/case management	The system will allow users to record multiple queries against one customer record
FR -004	Enquiry/case management	The system will record queries received through an online form (webform/e-form)
FR -005	Enquiry/case management	The system will enable users to track progress of customer query (set up of business process workflows)
FR -006	Enquiry/case management	The system will enable users to categorise queries by type, status, time received, channel of communication
FR -007	Enquiry/case management	The system will enable users to assign a query to a Customer Officer
FR -008	Enquiry/case management	The system will allow users to create a bespoke view
FR -009	Enquiry/case management	The system will alert users about an upcoming or overdue query
FR -010	Managing customer information	The system will allow users to access, view, edit and share information about customer(s) and their queries
FR -011	Managing customer information	The system will record the time/day when a is query received
FR -012	Managing customer information	The system will store electronic documentation against a customer's record/case
FR -013	Managing customer information	The system will provide a single customer view which will allow users to see all interactions and engagement by a single customer/case across the Customer Team Service
FR -014	Data confidentiality	The system will enable users to set up a security model based on user privileges
FR -015	Communication	The system will enable users to respond to customer queries

FR -016	Reporting	The system will provide Management Information on performance against SLAs/KPIs
FR -017	Reporting	The system will provide operational day to day Management Information
FR -018	Data Governance	The system will allow data to be pushed into PowerBI
FR -019	Customer Service	The system will enable users to ask a customer for feedback and be able to respond to the feedback
FR -020	Data Integrity	The system will enable all customer information to be consistent and correct
SEC-01	Security	All application data & user credentials must be encrypted. Emails should be encrypted with TLS 1.
SEC-02	Security	All PINS data should be encrypted at rest with AES-256.
SEC-03	Security	Consumer data, and the assets storing or processing it, must be protected against physical tampering, loss, damage or seizure.
SEC-04	Security	Separation must exist between different consumers of the solution to prevent one malicious or compromised consumer from affecting the service or data of another.
SEC-05	Security	Solution provider staff should be subject to personnel security screening and security education for their role. We ask for any staff used by a supplier especially those designing and implementing with Administrator roles to be SC cleared anyone working in the office without Administrator roles should be at the very least BC cleared.
SEC-06	Security	The solution/managed service must ensure that each individual user will have their own authentication credentials.
SEC-07	Security	The solution provider must have a security governance framework that coordinates and directs the overall approach to the management of the solution and information within it. Preferably Cyber Essentials Plus or ISO27001
SEC-08	Security	The solution/managed service shall allow for different levels of interaction with the data (e.g. No access, read-only, read/write, full access) per user or group of users.
SEC-09	Security	The solution/managed service shall only allow users to perform functions for which they are authorised.
SEC-10	Security	The solution should allow for application access rights to be allocated by Active Directory group membership.
SEC-11	Security	The solution should be designed and configured to identify and mitigate security threats.

SEC-12	Security	The solution should be subject to annual penetration testing by CESG CHECK accredited provider.
SEC-13	Security	The solution shall ensure that document content uploaded to the solution shall be virus checked. If content uploaded to the solution is found to contain a virus it shall be rejected. Subsequent scanning of existing content to be defined.
SEC-14	Security	The solution should prevent a single user ID from being used to invoke multiple sessions.
SEC-15	Security	The solution must be able to securely destroy all Information provided or created under any agreement and no longer required to be retained.
SEC-16	Security	Data must be held in the UK, EEA or countries with Adequacy Decisions Adequacy decisions (europa.eu)
AFS-01	After Sales Service Management	24x7 service desk for Severity 1 tickets (system unavailable for use) – 30 minutes
AFS-02	After Sales Service Management	Mon-Fri 0900-1700 UK time (excl bank holidays) for other severity tickets.
AFS-03	After Sales Service Management	Regular account reviews to include monthly contract management meetings between the supplier and the Inspectorate at which performance will be reviewed in line with Service Offering. To be held either virtually or at the Buyer's Main Address at Temple Quay, Bristol.