Be Rota Limited
Information and Security Measures
Schedule 1

---

1. Urgency Categories

Any Technical Issues reported by the Customer via the helpdesk shall be categorised by the Provider as follows:

a. Urgent: Technical Issues which cause a significant outage to a mission critical business function with no possible workaround;

b. Non-urgent: Technical Issues which are not categorised as Urgent or Emergency;

c. Emergency: Technical Issues which are reported by the Customer out-of-hours which can be categorised as Urgent,

each as further described in paragraph 2 below.

2. Urgency Definitions and Responses

2.1 The Provider and the Customer shall report and respond to Technical Issues as follows:

Type of Support required	Definition	Action	Timing	Response time
Non-urgent	Non-urgent Technical Issues including features of the platform which do have temporary workarounds including: • inability to download or upload data • Feature function failure • Candidate Mobile App failure	The Customer should submit a support ticket via the support portal, including screenshots evidencing issue.	Business Hours	24 Business Hours
Urgent	Urgent Technical Issues are those which cause a significant outage to a mission critical business function with no possible workaround such as • Log-in to the Site Manager or Resource Network Manager Application • Request staff • On-shift issues (e.g. clock-in/out)	The Customer should submit an urgent support ticket via the support portal, including screenshots evidencing issue.	Business Hours	6 Business Hours
Emergency	Out-of-hours major issues, or escalated major issues	The Customer should submit an Emergency support ticket via the support portal, including screenshots evidencing issue.	Business Hours	3 Business Hours

2.2 Notwithstanding the provisions in previous Section 2., the Provider shall use reasonable endeavours to:

a. seek to resolve all Non-urgent Technical Issues within 7 Business Days of reporting by the Customer;

a. seek to resolve all Urgent Technical Issues within 24 Business Hours of reporting by the Customer.

3. Security Measures

This Schedule outlines the Provider's current Security Measures. The Provider may vary its Security Measures at any time without prior notice to the Customer so long as it maintains a comparable or better level of security. This may mean that individual Security Measures are replaced by new Security Measures that serve the same purpose without diminishing the level of security to the Customer.

4. Data Classification, Storage, Transfer and Retention

The Provider has adopted the following Security Measures in relation to data classification, storage, transfer and retention:

a. Data (including Personal Data) ("**Data**") is collected by the Platform from the Customer and its Users in order to provide the Services.

b. Data is classified in accordance with the Provider's "Information Classification Matrix and Handling Guide" ("**Data Classification Guide**"), available at Appendix 3, and is automatically encrypted for storage on the Platform.

c. Data is stored in live environments at [S3 AWS data centres] located in London. If any Data is required to be stored on mobile devices for particular purposes, it is removed as soon as that Data is no longer required.

d. Data is transferred from the Hosted Services to the data centres using encrypted connections.

e. Data is automatically backed-up daily. Data cannot be deleted except by a senior member of the Provider's IT team with specific authorisation.

5. Platform Access

Access to the Platform via the Hosted Services is regulated as follows:

a. Each user of the Account has individual log-in credentials comprising a username and password to access the Platform via the Hosted Services ("**User**").

b. Data made by each User on the Platform, including the actions they undertake, are logged to each User and such information can be accessed on the Platform.

c. The Provider removes Accounts when a customer or User no longer needs access to the Platform (or a particular part thereof).

6. Security Incident Management

The Provider's security incident management procedures follow a disaster recovery pattern including a three-phase approach:

a. Detection of an incident;

b. Mobilising a specialised team to address the detected incident; and

c. Conducting a "post-mortem" and deep root-cause analysis of the incident.

The Provider's customer support team will be notified of any detected security incident which may impact the Customer's experience of the Hosted Services.

The Disaster Recovery Policy is followed for serious incidents.

The Provider does not deal with data centre and hosting incidents which are dealt with by its cloud services provider, AWS.

The Provider logs and monitors network traffic events to ensure that the Platform and related technology are secure. AWS provides tools to enable the Provider to do so.

7. Security Protection

The Provider conducts a security review on a quarterly basis.

AWS provides security capabilities and services to increase privacy and control network access as follows:

a. Network firewalls built into Amazon VPC, and web application firewall capabilities in AWS WAF let you create private networks, and control access to your instances and applications;

b. Encryption in transit with TLS across all services; and

c. Connectivity options that enable private, or dedicated, connections from your office or on-premises environment.

AWS Platform-as-a-Service provider Heroku uses a number of additional security features:

a. Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are permitted based on business needs. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

b. Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

c. Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

d. Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

e. Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Logging and monitoring are also used to ensure our technology is secure. AWS provided tools CloudTrail and CloudWatch enable us to see exactly what is happening in our AWS environment.

Visibility into API calls through AWS CloudTrail.

Log aggregation options, streamlining investigations and compliance reporting.

Alert notifications through Amazon CloudWatch when specific events occur or thresholds are exceeded.

Physical protection is provided by only allowing authorised Provider staff to access administration systems on a need -to-use basis. These users must use password-protected equipment and SSL/SSH encrypted connections into any administrative systems, preventing any non-authorized user from gaining access.

8. Risk management

The Provider's Chief Operating Officer is primarily responsible for risk management. The Provider conducts:

a. An internal risk analysis twice per annum.

b. A risk assessment of external partners/suppliers/contractors when initially engaging with such third parties and thereafter annually.

All of the Provider's agreements with third parties and employees include standard confidentiality provisions and the Provider undertakes background checks on employees at the time of employment.