BRADY POWERDESK - INFORMATION SECURITY PRACTICES

1. DISCLAIMER

The information contained in this document represents the current view of Brady as of the date of its publication. This document and its contents are subject to modification by Brady in its absolute discretion. Brady does not guarantee that the information contained in this document will be error-free or kept up to date after its publication. THIS IS AN OPERATIONAL DOCUMENT AND NOT LEGALLY BINDING. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BRADY MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, ABOUT THE INFORMATION CONTAINED IN THIS DOCUMENT.

2. INFORMATION SECURITY PROGRAM

Brady maintains an Information Security Program which includes appropriate physical, technical and administrative safeguards to protect any client data or confidential information ("Client Data") from unauthorized or unlawful destruction, loss, alteration, disclosure or access. Further, Brady maintains various policies including Information Security Policy, Acceptable Use Policy, Incident Management Policy etc., with objectives and targets set and monitored to achieve continual improvement of Information Security Program.

3. TECHNICAL CONTROLS

Brady maintains, where appropriate, certain technical controls to ensure the security of Client Data, including but not limited to, access controls, network controls, encryption, two-factor authentication etc. However, the internet is an open system and Brady does not warrant or guarantee that third parties cannot or will not intercept or modify Client Data outside of the application.

4. DATA BACK UP

Client Data will be backed up on a frequency appropriate to ensure the Recovery-Point-Objective (RPO) as detailed herein. Client Data backups will be stored within the same geographical region (but different data centre) as the rest of the Client Data, so as to preserve data residency and compliance boundaries. Brady may from time to time test its backup systems and may use copies of Client Data as part of these tests. In the event of a disaster, RPO will be a maximum of fifteen (15) minutes.

5. MONITORING

Brady will use reasonable endeavours to monitor the cloud solution 24/7/365 days per year. This will include automated alerts on the availability, welfare, performance and security of the components comprising the cloud solution.

6. INCIDENT MANAGEMENT

Brady maintains a Business Continuity / Disaster Recovery Plan to ensure business operations' continuation during an emergency, natural disaster, or cybersecurity threat. Brady will test such plan periodically at its discretion to ensure the effectiveness of the plan. If any breach of Brady's Information Security Program leads to the accidental or unlawful or unauthorized destruction, loss, alteration, disclosure of, or access to any client's data or confidential information (each a "Data Breach Incident"), Brady will investigate such Data Breach Incident, and subject to verification, promptly notify the affected client(s). The notice will summarize the nature and scope of the Data Breach Incident and the corrective action already taken or planned by Brady. Brady will take all reasonable actions to mitigate the Data Breach Incident. Brady will reasonably cooperate with affected client(s) in the investigation and remediation of the Data Breach Incident.

7. HOSTING PARTNER SECURITY PRACTICES

Brady utilises services from Microsoft Azure to host PowerDesk solution. Microsoft Azure follows ISO27001 and SOC 2 Type 2 certifications and other industry standard security practices. More information about Microsoft's security compliance can be found in the following link.
https://azure.microsoft.com/en-us/resources/microsoft-azure-compliance-offerings/

8. INFOSEC POINT OF CONTACT

Brady's primary information security point of contact is:

Mark Chadwick
IT Security Engineer
Brady Technologies Limited
Vision Park, Victory House, Chivers Way
Histon, Cambridgeshire, CB24 9ZR
mark.chadwick@bradyplc.com