Data & Security

Description	**Data & Security Information**
Author	**Sarah Bolton**
Version	**2.0**
Version date	**20th September 2021**
Policy Ref	**PP-SO010**

Overview

The following is an overview of the security measures currently in place, protecting both our hosted environments and the Point Progress offices.

Data Centres & Servers

- Consistent and compliant with the board principles of BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ITIL and best industry best practice and Service Continuity BS25999.
- UPS and diesel generator power systems – The servers are not reliant on the local power grid to guarantee around-the-clock power. On-site diesel-powered generators and uninterruptible power systems (UPS) deliver redundant power if a critical incident occurs. This ensures all operations are uninterrupted and the dedicated servers remain online.
- Redundant climate control systems – The heating ventilation air conditioning (HVAC) systems have full particle filtering and humidity control. The climate within the data centre is maintained according to ASHRAE Guidelines. This ensures that the mission-critical dedicated servers and hardware is functioning at its best.
- Fire Suppression – VESDA detection with clean agent fire extinguishers
- The data centres are locked and guarded – can only be accessed by authorised personnel.
- Monitored closed circuit televisions and 24x7x365 onsite security teams vigilantly protect the data centre, while military-grade pass card access and bio metric finger scan units† are in place to provide even further security.
- The data centres are multi-level low-rise building with a raised floor.
- 24x7x365 NOC Support Network Operation Centres (NOC) supplies 24x7x365 support. The NOC monitors the network, while engineers and data centre personnel keep the facilities running smoothly. Around-the-clock access to phone and online support is also available.
- Firewalls – protecting servers and mission-critical data from malicious traffic

Backup

- Local SAN storage
- Daily whole server backups
- Replication of whole virtual servers to an off-site location
- Data is backed up and encrypted, and transferred to SAN on secondary data centre
- Blade technologies are being used across all servers to increase data reliability

Monitoring

- Smart Monitoring allows us to identify and remedy any problems before they become visibly problematic
- Bi-Weekly Vulnerability Scans – the servers are vulnerability scanned using by Control Scan providing an audit of server security.

Version	Date	Description	Approved By
2.0	20/09/2021	Policy Redrafted	