Data Protection and Retention Policy

SSG operate a secure and responsible data protection and retention policy in line with governing organization requirements around all information and data considered sensitive, personal or required for proof of operations for auditing reasons.

The following procedures must be implemented which any data, which is considered sensitive, personal or required for, proof of operations for auditing reasons;

- Paper copies of documents must be in locked cupboards, cabinets and draws or in locked rooms. All areas must only be accessible by authorized personnel.
- Data that is stored electronically must be done so on equipment which is password protected. All areas must only be accessible by authorized personnel.
- Data that is stored electronically must have a full proof back up system to support the safe storage of this data.
- Paper copies of documents no longer required for use and do not need to be retained for record keeping/evidencing for audit must be shredded and sent for incineration.
- Paper documents that are required to be kept for record keeping/evidencing for audit or other purposes must be stored in an archived system using an effective and reliable archive system, and kept in a safe and secure location.