IT DR Policy

Prepared for:

in2skills

0844 32 40 970 | sales@SITOC.com | www.SITOC.com

Company Registration Number: 05278300| 4 Gleneagles Court, Brighton Road, Crawley, West Sussex, RH10 6AD

1 DOCUMENT PURPOSE

This document is intended as a high-level summary of the technical and procedural measures in place for IT network protection, Disaster Recovery and Cyber-attack response at in2skills (referred to as I2S herein).

All content is correct at the time of printing and is reviewed/updated in-line with IT change management and security review policies. The primary contact for any queries relating to this document is your account director: miles.fisher@sitoc.com

2 DISASTER RECOVERY – PREVENTATIVE CONTROLS

I2S maintain an IT security blueprint across all locations and user hardware, this includes the following services which are deployed, maintained and supported by an external specialist MSPP (Managed Service & Security Provider), SITOC Ltd. These measures are in direct support of data protection and disaster recovery resilience.

1. **Security patch/firmware management & Asset control -** An enterprise-grade solution is used for the remote control, security management and housekeeping duties associated with workstation and server hardware.

   This tool (Kaseya) is also used for the following regular tasks:

   - For secure remote access to workstations for planned/non-planned works and diagnostics, controlled by 2FA.
   - Managed deployment of firmware updates and patches to all workstations, this process includes prior sandbox testing to ensure that all releases are compatible, and, do not cause any adverse effects. Examples include Windows updates and emergency security patches. A central log is maintained of all firmware updates and deployment success/failure. This process forms a critical part of network security and ensures that any vulnerabilities are closed off.
   - Regular removal of unnecessary & temporary files by means of "flushing" areas such as DNS logs and other temp file locations. This is in an effort to reduce bloating of hard drives and maintain the maximum life expectancy of hardware
   - Application standardisation by means of scripted rollout. This ensures that all users are kept at a harmonious level in regard to application versions and maintains the effort to enforce standardisation in IT network design. Other examples of

centralised rollout include the deployment of new print drivers and general scanning tasks.

- Asset management, by means of applying a unique identifier against each hardware device, therefore complete visibility of all network assets and meta data (such as make/model, network location, last activity/login time, applications installed etc.)
- Network scanning, to identify rogue or unauthorised devices.
- Notification of failed password attempt at workstation level
- Removal of unnecessary software or "bloatware" by means of deploying a standardised build configuration onto all new workstations

2. **Anti-Malware:** Administered and monitored by a SITOC, each workstation is deployed with **Webroot SecureAnywhere** business protection applied. As a centrally managed and cloud-based platform (integrated with Kaseya via API) this ensures that the entire group is protected with a single/consistent solution with automated alerts of any significant activity. In addition to virus/malware/crypto protection the service also provides online protection by means of keylogger detection, keystroke encryption and malicious site detection.

3. **Web & DNS protection:** This service provides an additional layer of network security by means of internet restriction & monitoring capabilities. Powered by Webroot as an add-on to anti-virus (see prior section) users are protected from harmful sites/content and allows for the restriction of websites by category, reputation or specific URL.

   As a DNS based solution, this service also provides protection against threats such as cache poisoning, DDoS, DNS hijacking, botnets, C&C and man-in-the-middle attacks.

4. **Firewall:** I2S operate a comprehensive strategy for firewall deployment, management and remote access. Fixed locations (currently Haig House, Hastings) are protected by means of a CISCO ASA firewall appliance; the hardware is currently vendor-supported and firmware updates are deployed as part of the aforementioned outsourced Managed Service & Security contract.

   A CISCO-CISCO VPN is in place for communication between group offices, note that remote access is permitted only from trusted devices outside of the network (such as home/remote workers) and only be means of desktop VPN which is deployed and controlled centrally. Notwithstanding these controls, each request for remote access follows a strict internal policy whereby a documented business case may be required

before approval is granted. Such alterations fall under the general change management policy.

As per industry best-practice, all default firewall usernames and passwords are changed prior to deployment (and held in a hashed & encrypted format), furthermore, router and firewalls are configured to prevent internal services being "advertised" externally.

5. **Access & Password management:** SITOC control password and access management on behalf I2S, this includes the following measures:

   - Routine and forced password resets, with strict rules on character length and complexity
   - Enforced multi-factor authentication, such as when remotely accessing Office 365 services
   - Network access audits
   - Secure password sharing by means of proprietary secure messaging service (powered by Mimecast)
   - A secondary means of identification is required before sensitive request are carried out. For example, if our service team receives a sensitive change request via email, we shall phone for verification, and vice versa. Such request are also "scored" against granted permission levels.
   - Regular review of all network logins for validity, including access rights i.e. what user privileges are in place, and, are they still relevant

A strict leaver & joiner process is in place to maintain the above, this encompasses a series of questions which must be answered fully before action is taken. For example, when a new staff member joins I2S we must establish what permissions they should have, or, what should be revoked when they someone leaves the organisation.

6. **IT policy –** All systems, services and procedures detailed herein are supported by a range of written IT usage and data security policies. These form part of employee induction training and affirm the acceptable use of IT services/internet/email, IT risks, escalation procedures amongst general data security education.

   These policies are compiled/updated in accordance with legislation and are reviewed on a regular basis.

7. **Training and education –** All staff are coached in the use of the IT systems at I2S, and, are required to familiarise themselves with the IT policies in place. Ongoing security awareness training is also provided.

8. **Backup** – I2S maintain a comprehensive data backup solution which is administered and monitored by SITOC.

This cloud-based service provides the ability to easily restore an individual file and/or entire file structure or database. Backups run daily and are held in a private UK cloud platform, note that this is disparate from primary Microsoft 365/Azure data hosts in accordance with best practice i.e. to host backup data within a separate platform and data centre host.

Retention periods vary from 60-90 days and can be extended if required. The service is designed to provide effective recovery from individual file deletion (whether it be malicious/accidental or become corrupt), or entire server failure. This solution also provides an effective countermeasure to Crypto locker-style attacks and ransomware in addition to the anti-malware protection already in place.

SITOC monitor backup completion status as part of the managed service agreement in addition to the recovery of files as and when required.

3 DISASTER RECOVERY – REACTIVE CONTROLS

I2S understand the responsibility to prepare for a DR event or cyber-attack despite investment in the preventative measures noted prior.

A varying range of response actions are taken following an event (either through event monitoring or staff alert). Response is administered via SITOC ltd, with a 24/7 response facility maintained.

Event process is summarised as follows:

1. Relevant managers are notified of the issue (via email and/or telephone). Summary details of the issue, where to view updated and who to contact for progress is also shared.

2. Root cause analysis is used to firstly identify affected services. This is achieved by using email/server/desktop security tools to highlight affected services, some of these may be retrospectively deployed based on the nature of the event.

3. In the event of workstation/server compromise these machines shall be moved into quarantine both virtually and physically by removal from the internet and LAN.

4. Line mangers shall be in the event of suspected malicious employee activity (where identified under root cause analysis)

5. Restoration of service and recovery time shall vary based on the event, however, the following measures are typically utilised:

    - PC/laptop quarantine and restoration (only where individual users/workstations are affected)

    - Limitation of internet access to voice-only communications where a site-wide threat exists

    - External services may be taken offline where affected (such as websites)

    - Invocation of DR services, such as failing over to hot-standby server and/or restoration of primary server by use of backup image

    - Running of threat-specific tool to perform retrospective fix (dependent on event)

    - Provision of remote/mobile working facility for key-staff where the estimated time to fix is significant

    - Relevant authorities shall be notified where root cause analysis or genuine "warning message" from the attacker identifies that personal data has been copied and/or any individuals may be at risk (whereby the police will be notified).

      As a further measure, the Cyber-security division within the NCA may also be notified however this is typically treated as a secondary measure, post-event.

Where no evidence of data compromise is evident, the following close-down and post-event actions usually take place.

- Return of equipment to end-users and/or services resorted to primary server in the event of standby image being invoked

- Incident report generated by 3rd party provider and shared with senior management. This includes any available information such as entry-point,

execution/spread and remediation. A sub-set of this report shall be circulated to all employees in an effort to spread awareness and provide education.

- Existing IT policies and training sessions are reviewed and updated if required
- Existing IT security services shall be reviewed in direct correlation to the event
- Reports and findings to be shared with relevant regulators if required (such as the ICO).
- Where an attack has taken place via an external infrastructure/software host or data processor (i.e. outside of company control) I2S shall review any post-event reports and RFO's in-line with company policy.