

Logging and Monitoring Policy

This document provides details of the Company's logging and monitoring of its internal systems.

Scope

All servers and systems that contain client or other sensitive data.

Responsibilities

The IT Director will be responsible for the monitoring of this policy. QRS outsources its IT Support (currently Assign-IT) who will monitor its policy and provide any necessary information to QRS to meet its responsibilities.

Policy

QRS Market Research will monitor any system that may contain client or other sensitive data.

Event logging shall be undertaken every 30-45 days unless there is a suspicion of anomalous behaviour. SharePoint logs shall be used to identify suspicious behaviour with failed login attempts reviewed. Confirmit shall be asked for logs of failed login attempts to both the interviewer and professional platforms. A log that the event logs have been reviewed shall be kept by the IT Director. This document will keep a record of the date of review, any suspicious events identified and the result of the follow up.

Event logs shall be stored within SharePoint for a minimum of 60 days. Confirmit will store event logs for 45 days.

The following will be monitored:

Server/SharePoint:

- CPU / Memory / Disk capacity
- Successful and Unsuccessful logon events
- Account Creation and deletion activities
- Audit of access to sensitive areas of storage

CATI:

- Successful and Unsuccessful logon events of CATI workstations
- Unsuccessful logon event on the CATI application

Email:

- Successful and unsuccessful logon event recording email address and location of IP and User agent

- Admin attempt to forward emails
- Creation of new mailboxes/users

All logging locations will be configured to use NTP as a time source to ensure that all logged events can be correlated if required.

All incidents are logged and detail the following:

- Incident/event type
- Incident/event description
- Detection method
- Severity rating
- Corrective action taken
- Preventative action taken