ramsac

Internal security practices

ramsac

the secure choice

Environment

Core business tools

ramsac's core business platforms are provided by an industry-leading technology provider for MSPs (Managed Service Providers). ramsac use PSA (Professional Services Automation) software as our Support, CRM (Customer Relationship Management), order processing and invoicing system. We also use RMM (Remote Monitoring & Management) software to manage our client's workstations and servers.
Our primary email and content management systems are hosted with Microsoft and fully secured to industry standards. All employee accounts for these platforms are secured with MFA and sign-in logs collected.

These systems contain personal (client contact names and business contact details) plus technical information about our client's environments. Access to systems, and data within them, is fully controlled with Principles of Least-Privilege (PoLP). We are very much aware of the sensitivity of this information, hence why security of our systems and data is our number one priority.

Security systems

ramsac have deployed a number of security tools and measures to safeguard against cyberattacks. ramsac deploy enterprise-grade Anti-Virus, email spam filtering and Firewalls to protect against malware and network intrusion.

We utilise our own secure+ services to continuously monitor for signs of cyberattack or data leakage. We make full use of Microsoft security recommendations to control devices, harden our estate, and reduce our attack surface.

Artificial Intelligence (AI)

ramsac have an AI policy which all employees are required to adhere to. All employees receive training around AI best practices and how to use AI ethically and appropriately. AI tools are currently used in limited capacity across ramsac, following stringent data and security checks.

All AI tools in use at ramsac hold ramsac and ramsac-client data in logically separated tenants and language sets which are not shared across the internet or with other clients/3rd parties.

Devices

All staff use ramsac provided laptops which are encrypted with BitLocker and are monitored as part of our totalIT service. Staff are also trained not to save personal or sensitive data locally, even on ramsac owned devices. Our Information Security policy bans accessing corporate data on personal laptops or desktops. Corporate data can only be accessed on mobile devices through the official Microsoft apps which containerise the data and allow us to remotely wipe data from devices in the event the device is lost or stolen.

Employee security

Staff identity verification

All staff with access to systems which contain client data are contracted members of staff and employed directly by ramsac. For ramsac staff we take two references from previous employers/educational establishments, or a character reference if two aren't available. We verify new starters identity by checking their passport, which we scan and store in our HR system.

Staff training

All staff undertake security training as part of their induction, which covers our Information Security and IT Acceptable Use policy with a focus on the sensitivity of the information in our key business systems, and likely current threats to ramsac and our clients. All staff are also required to undertake monthly online Information Security training. We monitor compliance and ensure that all staff, without exception, are up to date with training.

All staff undergo a thorough induction and training programme on all systems, with technical staff spending several months shadowing an experienced member of the team before working on systems unsupervised. Phishing testing is conducted on a regular basis to identify any areas of risk where additional training may be required.

Access to systems containing client data

Staff are only given access to key business systems that contain client data according to their job role. Access to information within these systems is further restricted, for example limiting access to invoices for non-finance staff. In particular we restrict access to domain and Microsoft 365 tenant administrative passwords to technical staff with a need to use that information.

We further avoid the use of Microsoft 365 tenant administrative credentials by technical staff by using our Microsoft 365 Cloud Service Provider portal provided by Microsoft. This also provides us with a better audit trail, as users log-in with their own ramsac credentials rather than tenant admin credentials.

Verification of changes

For all clients we require a list of staff who are authorised to make changes which may have security implications, such as password resets, providing access to folders or mailboxes, new account creation etc. Our support team will always obtain authorisation from an authorised contact before proceeding with any of these changes.

Some clients use a text message based system for password resets, where we will send a new password only to the mobile number we have been provided in advance.

Accounts, auditing & GDPR

Accounts

In addition to complex passwords which are changed periodically and not re-used between systems, multi-factor authentication is used for all business systems.

Leavers accounts are disabled and all kit collected before they leave the building on their last day at ramsac.

Auditing, testing and incident process

We are certified to the Cyber Essentials standard and are in the process of becoming certified to the ISO27001 and Cyber Essentials PLUS standards.

We conduct regular vulnerability scans and subscribe to a range of reporting services that give us early warning of potential vulnerabilities that could impact ramsac or our clients.

ISOQAR REGISTERED

UKAS MANAGEMENT SYSTEMS 0026

Cert No. 2921
ISO 9001

As mentioned above we use our own secure+ service which enable us to monitor for signs of a potential cyber breach. This service is managed by a dedicated Cyber Security team who take action on any suspicious activity or incidents.

We have a documented incident process which gives both staff and managers immediate actions in the event of an incident and sets the agenda for an incident meeting involving the ramsac Senior Leadership Team.

We have a documented Business Continuity Plan which is tested on a regular basis.

GDPR

We are comfortable that we are compliant with GDPR, having had an external audit by a GDPR specialist and undertaking annual internal audits. We have documented third-party processor agreements with all relevant providers.

GDPR

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice