ramsac

Internal security practices

ramsac
the secure choice

Environment

ConnectWise Manage

We use ConnectWise Manage as our support, CRM, order processing and invoicing system. ConnectWise Automate is our RMM system (remote monitoring and management of client desktops and servers) and Microsoft 365 for e-mail, document storage, communication, collaboration and identity management. All of these systems require MFA for all accounts.

Manage contains both personal information (client contact names and business contact details) plus technical information about our client's environments, including administrative passwords, firewall and router credentials and configurations. We are very much aware of the sensitivity of this information, as well as the risks around Automate being compromised.

We do not store other customer data on our systems. All data storage and backup solutions used by our clients are hosted by reputable providers, with complete transparency around the provider and hosting location.

Azure Active Directory

We use Azure Active Directory, there is one remaining physical server in our Godalming office for our phone system. We use conditional access in Azure AD, which restricts access to the Microsoft Outlook app on iOS and Android devices, giving us remote wipe capability of both Outlook and OneDrive/ SharePoint data.

secure+ from ramsac

We use our own Secure+ service, which is based on the Microsoft Sentinel SIEM to monitor and respond to threats to both our on-premises and Microsoft 365 environment.

Sophos Intercept-X

We use Sophos Intercept-X as our anti-malware/EDR platform, and Mimecast for e-mail security. Mimecast re-writes URLs in e-mails so they can be assessed by Mimecast if they are clicked, and all attachments are replaced with safe PDF versions to reduce the risk of malware.

Employee security

Staff identity verification

All staff with access to ConnectWise Automate are contracted members of staff and are 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 Manage and Automate, and likely current threats to ramsac and our clients.

All staff are also required to undertake monthly online information security training, which includes a short quiz at the end of each session. 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, for technical staff spending several months shadowing an experienced member of the team, so are well trained on Manage and Automate before working unsupervised.

Phishing testing is conducted on a regular basis to identify any areas of risk where additional training may be required.

Access to ConnectWise Manage and Automate

All staff require access to ConnectWise Manage, however access to information is restricted based on job role, for example no access to invoices for non-finance staff.   In particular we restrict access to domain and Office 365 tenant administrative passwords to technical staff with a need to use that information.

We further avoid the use of Office 365 tenant administrative credentials by technical staff by using our Office 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.

Access to Automate is restricted to technical staff with a need to use the system. Full logging is in place, with multi-factor authentication on all accounts.

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 Manage, Automate and Office 365.

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

Auditing, testing and incident process

We are certified to the Cyber Essentials standard (see attached certificate) and are in the process of becoming certified to the ISO 27001 standard.

We conduct an external vulnerability scan on a weekly basis and subscribe to the NCSC Early Warning weekly vulnerable service report, which flags up any vulnerable services identified by an NCSC scan of our external IP range.

ISOQAR
REGISTERED

UKAS
MANAGEMENT
SYSTEMS
0026

Cert No. 2921
ISO 9001

As mentioned above we use our own Secure+ service which gathers logs from on-premises servers, firewalls and from Microsoft 365 and analyses these in Microsoft Sentinel. We have a dedicated Cyber Security team who monitors and takes action on any suspicious activity or incidents.

As mentioned above we undertake regular phishing testing (at least six monthly)

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 (a redacted copy of this plan is available on request)

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

Devices and change verification

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.

Devices

All staff use ramsac provided laptops which are encrypted with Bitlocker, which is 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. As mentioned above our conditional access policy blocks use of any mail client other than Microsoft Outlook on mobile devices, which we can then remotely wipe in the event of loss or theft.

All ramsac laptops use a VPN which directs all traffic via our Godalming office network and firewall.

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice