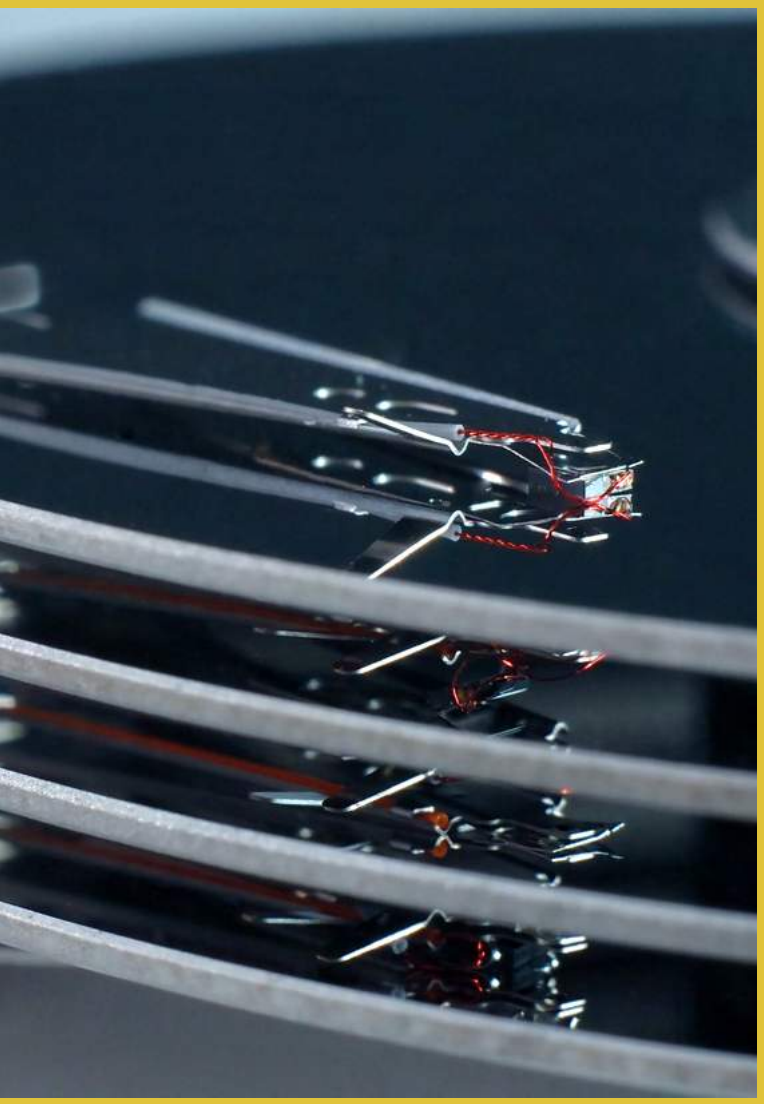
SUPPORT SERVICES

Infrastructure security

enable®

Introduction

Enable's commitment to the most stringently tested security does not stop with application security, as the threat of an attacker gaining access to a server either physically or remotely, can be potentially devastating.



Infrastructure security is another vital part of the overall security equation at Enable and is reflected throughout our business from our working practices and the training we give our staff to our IT infrastructure and the technologies that we use on a daily basis.

This document describes the various types of infrastructure safeguards that Enable provides to ensure that we have a solid and secure foundation on which to build our high-quality software and protect our clients from attacks that can result in loss of revenue and reputation.

Company practices

Part 1
Overview

The security of our infrastructure is the shared responsibility of everyone at Enable and not just our IT team. While there are many significant measures that employees will be aware of, such as physically protecting our infrastructure using firewalls and antivirus software, there are also other extremely effective company practices that are implemented to fully enforce infrastructure security at all times.

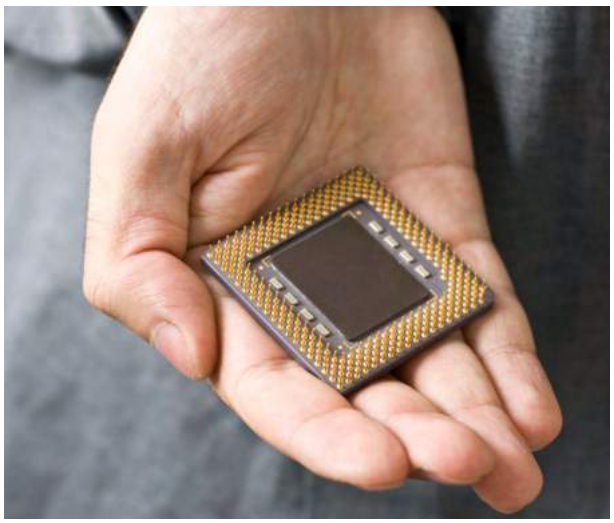
ISO 27001

ISO 27001 Information Security is a standard of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. Companies that meet the standard after a successful formal compliance audit are certified compliant by an independent and accredited certification body.

Enable has successfully achieved these accreditations which recognise the robustness and quality of the information security management systems that we have in place. The accreditations also demonstrate Enable's promise to maintain confidentiality, integrity and availability of information security while managing business continuity and minimising business damage by preventing and reducing the impact of security breaches.

ACCREDITATION AND AUDITING

To maintain this accreditation, internal audits are undertaken at least once a year and an external audit is performed annually. Data protection is not audited separately but as part of the whole information security process. All results of information security audits are documented and reviewed at quarterly management meetings by the managing director, operations director, IT manager and the office manager. Any non-compliances or non-conformities found are recorded with relevant action decided on and a target date established.



Part 2
Personnel

PRIVILEGES

Any access to systems is controlled by the rule of least privilege and servers undergo hardening with antivirus software installed by default on all servers and workstations. System updates are also checked for on a regular basis and encryption is used where appropriate.

The IT team has access to the production systems and can authorise short-term access to resources for members of other teams where justification is provided, while access to the network, applications and VPN is only granted by the IT team upon request. The IT team are responsible for communicating log-on details for a new starter and ensuring that they have access to the company's policy on passwords.

We maintain complete segregation of duties between the support and hosting team and the software development team so as to ensure that those personnel involved in controlling code have limited access to production environments and/or live data.
All platform and data access permissions will be monitored on an ongoing basis in order to ensure only the relevant levels of access are granted.

MANAGEMENT REVIEW

On a quarterly basis, Enable holds management review meetings where any issues concerning privacy and potential breaches of information security are handled.

RESPONSIBILITIES

The managing director has overall responsibility for data protection along with the operations director. The IT manager ensures that all office systems e.g. computers, laptops are established and maintained to reduce the risk of breach to data protection while the office manager ensures that any breaches or risks are recorded and action taken where appropriate.

INDUCTION PROCESS

On induction to Enable, new employees receive awareness training on the importance of data protection. Any changes to policies and procedures are notified to all staff when these are made. Line managers are responsible for ensuring that identity checks are carried out on new staff in accordance with employment law and that records are maintained. References are sought for new staff and copies kept on file.

Contracts of employment and company policies are signed by all new staff to confirm their understanding and acceptance of the conditions. These contracts cover:

— Pre-employment checks;
— Non-disclosure obligations;
— Investigations and disciplinary controls.

All new starters undergo induction training in accordance with Enable's training policy with any assets issued recorded and signed for. They are also granted access to our information systems in accordance with the company's policy.

CHANGES TO ROLES

The relevant manager is responsible for notifying the IT manager when a member of staff is due to change role or terminate employment. The notification is made in writing or email and will clearly indicate the date of the change or termination. If the change of role results in a change to the person's access rights to the network or to any information systems, the IT manager will arrange for this to be done and an equipment issue form is used to ensure that all equipment originally issued to the employee is returned to the company.

Where employment is being terminated, the IT manager will use the former employee policy to ensure the securing of their domain account, email, files and documents on the Enable network and on their workstation. The IT manager will consider whether the change or termination of employment has an impact on information security, this includes the changing of any access codes to the building and passwords if necessary.

USE OF CONTRACTORS AND THIRD-PARTY ACCESS

Non-disclosure agreements (NDAs) are drawn up with our contractors and requests for third-party access to Enable's information systems or for unescorted access to the premises must be made to the IT manager in writing.

The IT manager is responsible for assessing the risks before an external party is granted access to Enable's information processing facilities or offices and access is only granted where it is necessary to provide a service. NDAs or Confidentiality Agreements are signed where the contract does not make explicit reference to confidentiality and the IT manager ensures that appropriate controls are in place and the external party cannot access unauthorised information.

A list of third parties who have signed NDAs or confidentiality agreements with Enable is maintained by the IT manager and is reviewed annually or when changes occur. The IT manager also ensures that third parties are made aware of Enable's information security requirements prior to granting access.

REVIEW OF ACCESS RIGHTS

On an annual basis, a review of all access rights is undertaken by the IT manager, the office manager and the operations director to ensure that rights are appropriate and up-to-date. These can include:

— User privileges;
— Access codes;
— Cloud services;
— Client environments;
— Supplier contacts.

A record that the review has taken place is also retained.

OFFICE ACCESS

A list of keyholders for the building is maintained and reviewed on an annual basis and whenever changes occur, while an electronic fob is required to gain access to the building when it is locked. Records of the issue and return of fobs are automatically logged. Non-Enable personnel are required to make an entry in the register in reception each time they enter or leave the building — confirming the date and time of their arrival and departure – and are accompanied by Enable personnel unless they are in rooms where no sensitive information is available.

During office hours staff also ensure that windows are closed and locked if the offices are unattended, even if this is only for a short time.

Part 3
Workplace and equipment

CLEAR DESK AND CLEAR SCREEN POLICY

Enable operates a clear desk and clear screen policy that requires users to ensure that unattended computers have their screens protected by a password-locked screensaver and that computers are always logged off and closed down at the end of the day. Desk areas are also not permitted to have any sensitive data on display when left unattended.

COMPUTER EQUIPMENT

Computer screens are positioned so that they won't easily be overlooked by any unauthorised personnel, e.g. through the windows.

Staff also ensure that cabling around and under their desks is tidied to prevent accidental damage but if any problems should arise with cabling this is immediately reported to the IT manager.

Computer equipment is never taken off-site without the authority of the IT manager and staff are always held responsible for ensuring that equipment and media taken off premises are never left unattended in public places or in vehicles unless locked out of sight. In case of portable computers, these are password protected, locked and disguised where possible when travelling.

All computers are assigned to an individual and a record is kept by the IT manager.

DISPOSAL

The IT manager is responsible for the secure disposal or reuse of equipment, including removable media, and ensures that any sensitive information and licensed software is removed as appropriate, while hard drives are isolated and damaged beyond use.

Where external parties are used to securely dispose of equipment or media, only approved suppliers are used and certificates of destruction or disposal are kept as appropriate.

A record is maintained of all equipment and media disposed of and the method of disposal.

PERSONAL DEVICES

Personal computers, laptops, phones, etc., are not used to process Enable's information without the authority of the IT manager and, once approved, data is still not permitted to be download onto the device.

VIRUSES AND MALWARE

Any user who suspects that their computer may have been affected by a virus or malware immediately contacts the IT manager, where a note is made of any messages or unusual behaviour. The computer is not used again until clearance has been given by the IT team who are responsible for restoring the computer to its prior state. If appropriate, the IT manager raises a non-conformance report.

Software can only be downloaded or installed in accordance with Enable's internal policies to ensure that the software is legal and does not pose a security risk, while complying with the relevant software licences. Firewalls and virus checkers are in place and are controlled by the IT manager and no removable media is used in any computer unless it has first been scanned.

MALICIOUS MOBILE CODE

The following measures are in place to protect against malicious mobile code:

— Software is not installed without the authority of the IT manager, who also ensures that all software licences are complied with;
— Virus checking software and firewalls are installed on all computers and also on the server, with updates being cascaded to the users with no intervention from the users being required;
— No media is inserted into any computer without it first being virus checked.

A user who suspects that their computer has been affected by malicious mobile code immediately contacts the IT manager and a note is made of any error messages or unusual behaviour. Here again, the computer will remain unused until clearance has been given by the IT manager who is responsible for restoring the computer to its prior state.

AUDIT LOGGING

Audit logs of users' activities and security issues are maintained by the computer system and the information is held securely and backed up on a daily basis.

Logs are retained for a minimum of six months or in accordance with any legal, regulatory or contractual obligations while all access requests are logged either by the application service or the underlying container platform. The minimum information recorded is as follows:

— Data and time of the request;
— Message authentication header digest;
— Service endpoint identifier;
— Client (requester) identity (e.g. user ID);
— Client (requester) source address;
— Server response (success) code.

FAULT LOGGING

Any faults with the information processing facilities are logged with the IT team and corrective action is taken where necessary with records kept for analysis.

CLOCK SYNCHRONISATION

The clocks of all information processing facilities are controlled and synchronised by use of the Network Time Protocol (NTP).

Part 4
Other considerations

BACKUPS

Enable has a tiered approach to its application and server backup process, which is as follows:

— Databases, fully, every evening;
— Database transaction logs, every four hours;
— App files, differentially, nightly;
— App files, fully, weekly;
— Cloud server images, weekly
— Backups are encrypted;
— Backups are not stored on source servers;
— Offsite backups are taken on a weekly basis;
— Backup procedures are reviewed quarterly;
— Backup procedures are monitored on a daily basis, or at an interval that is applicable to the backup's frequency.

EXCHANGE OF INFORMATION

Whenever confidential data is exchanged between Enable and an external organisation, a confidentiality agreement is in place.

ELECTRONIC MESSAGING

All electronic messaging is protected by a firewall and virus checker and email and internet policy is issued to staff at induction.

EQUIPMENT MAINTENANCE

Equipment maintenance and repairs are only performed by authorised personnel with the IT manager responsible for ensuring that approved suppliers are available to repair and maintain equipment. The office manager is responsible for the maintenance of supporting equipment, such as the air-conditioning and alarm systems, and records of servicing, maintenance and repair are maintained. Records of any suspected or actual faults and the preventive and corrective action taken as a result are maintained by the IT manager and, where appropriate, non-conformance reports are raised in accordance with company policies.

FAULTS

The IT manager is responsible for maintaining a log of IT faults, identifying trends and, where applicable, raising non-conformance reports.

CHANGES TO INFORMATION SYSTEMS

Any changes to Enable's information systems, including the addition of new systems, are reviewed, approved and tested prior to implementation, if appropriate.

Where testing is deemed to be necessary, this is done and recorded by the IT team while also ensuring that test systems and data are clearly identified as such and are not located in the same area as live systems and data. Sensitive data, live user IDs and live passwords are never used as part of the test and all results, including any remedial action, are recorded also. Once a change has been implemented, it is reviewed for effectiveness with particular emphasis placed on information security. All parties affected by the change are informed.

Preventative measures

Part 1
Safeguards

Being part of the connected world brings certain dangers as well as benefits as a computer that is connected to the internet is at potential risk from various security breaches and attacks such as viruses, Trojans and spyware. This section of the document gives an overview of the preventative measures that Enable takes to protect our clients' sensitive data and ensure the secure day-to-day running of our infrastructure.

FIREWALLS

A firewall is a network security system that acts as a barrier between a trusted and an untrusted network by controlling access to the resources and only allowing traffic defined in the firewall policy onto the network. Firewalls are used to protect all of Enable's servers and are configured to only allow access for the protocols necessary for that server's purpose - such as HTTP and HTTPS being allowed for web servers. Other protocols are only configured where required and filtered by an IP address white list if applicable – for example, only Enable administrative IP addresses may be permitted access. Furthermore, Enable team members' remote access to the servers is via Remote Desktop and is restricted to Enable administrative IP ranges.

ANTIVIRUS

Antivirus is computer software used to prevent, detect and remove malicious software. It was originally developed to detect and remove computer viruses, however, with the rise of other kinds of malware, antivirus software started to provide protection from other threats such as Adware and Ransonware. All of Enable's servers have a combination of Symantec Endpoint Protection and Sophos antivirus installed in order to protect against these threats.

RAID

RAID (redundant array of independent disks) is a data storage technology that combines multiple physical disk drive components into a single logical unit. This can be for the purposes of data redundancy and performance improvements or in some cases both. Data is distributed across the drives in one of several ways, referred to as RAID levels, and an appropriate RAID level is used to protect against the risk of hard drive failure depending on the required level of redundancy and performance. Below are some examples of the RAID levels that Enable uses.

RAID 1 — This consists of data mirroring without parity or striping. Data can be identically written to two or more drives in order to produce a "mirrored set" and any read request can be serviced by any drive in the set. If a request is broadcast to every drive in the set, it can be serviced by the drive that accesses the data first, improving overall performance.

RAID 5 — This consists of block-level striping where parity information is distributed among the drives — requiring all but one drive to be present to operate. RAID 5 requires at least 3 disks which means that the only way to lose the data is in the extremely unlikely event of two drives failing at the same time. This method also increases performance while at the same time providing redundancy.

RAID 1+0 — This is a combination of RAID 0 and RAID 1 which creates a striped set from a series of mirrored drives. The array can sustain multiple drive losses so long as no mirror loses all its drives, making it a more secure option. RAID 1+0 also benefits greatly from the rebuild time being very fast should a fault occur as all that is required is copying all the data across from the surviving mirror to a new drive.

INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. It regularly performs internal and external scans of a hosted solution with unlimited vulnerability assessments, while providing 24/7 monitoring of real-time threat alerts by security analysts. Enable does not provide IDSs as standard but it can be set up if it is required by the client.

SOFTWARE UPDATES

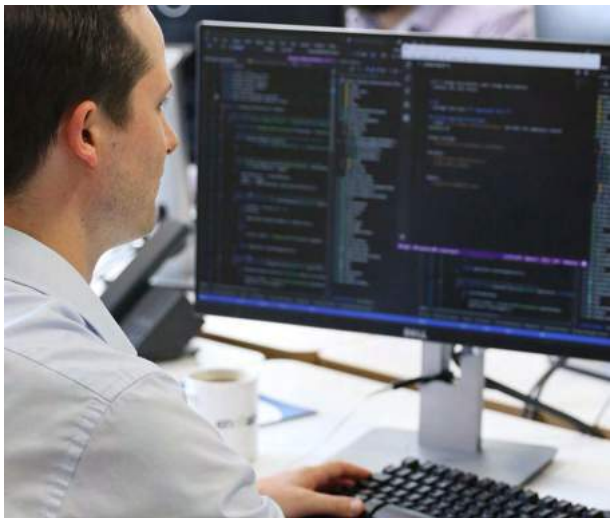
It's vital to keep software up to date as there will always be security flaws with any piece of software and it is often just a matter of time before an attacker discovers one. Enable's workstations and servers are manually updated on a weekly basis with preferences set to 'download but not install' so the IT team has the opportunity to inspect and decide which updates are required and to prepare for any downtime that these updates may cause. Updates are only applied once they have been manually approved. Updates to other pieces of software are reviewed on a monthly basis and their application to Enable's servers is only undertaken once they have undergone proper planning. Additionally, updates to application and web site code are performed only by authorised members of Enable staff once they have been fully tested and approved.

SERVER CONFIGURATION HARDENING

Server configuration hardening is the process of enhancing server security through a variety of preventative measures which results in a much more secure operating environment for the server. Enable's standard server hardening policy includes:

- Configuring reverse domain name system;
- Disabling NTLM;
- Disabling SSL 2.0;
- Ensuring strong SQL Server passwords;
- Configuring SQL Server connection auditing;
- Disabling weak ciphers < 128-bit;
- Removing standard HTTP headers;
- Ensuring AV is installed on servers;
- Ensuring IIS headers don't leak IP address;
- Disabling HTTP verbs that aren't required;
- Preventing ICMP response;
- Preventing download of .vbs and .bat files;
- Whitelisting outbound HTTP access;
- SQL Server Service user configuration;
- Ensuring custom error pages are displayed;
- Locking down IIS to SSL only;
- Running Windows updates.

In terms of industry standards or compliance with NIST standards, Enable has developed its own hardening standards as opposed to using industry standards.



Part 2
Communication protocols

WEB ACCESS, HTTPS AND SSL

Without exception, all communications with cloud based applications that require user identification and authentication are performed over HTTPS.

Enable owns and maintains the SSL certificates used and this is based on the assumption that the parent domain is the one for which Enable has responsibility.

SFTP

Secure File Transfer Protocol (SFTP) is a popular method of securely transferring files between two remote systems. Clients often need to exchange data between applications using file-based transfer models and typically these files would be either:

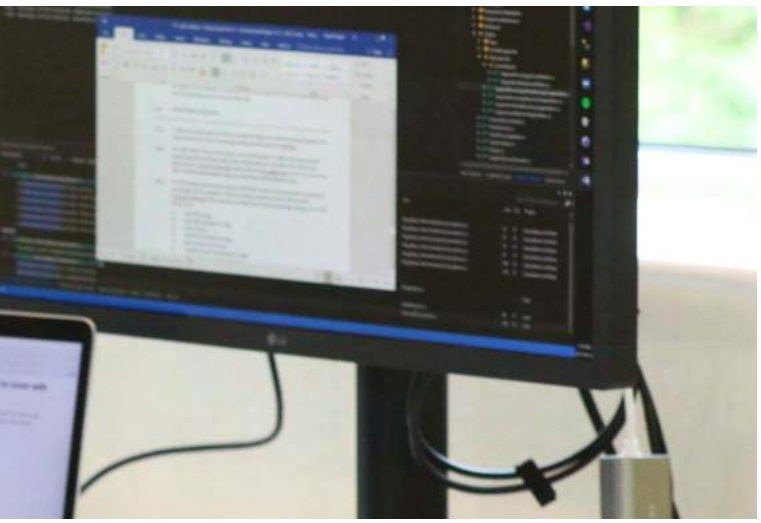
— Generated by a legacy system for consumption;

— Or, automatically generated for consumption by other systems, either on an event-based schedule, fixed routine or on-demand.

Enable recommends the use of SFTP for the transfer of these files and, typically, an SFTP facility will be provided by Enable within the relevant hosting environment with credentials then issued to the appropriate parties on a case-by-case basis. In addition to using encrypted communication protocols, the data files that are deposited or retrieved from the SFTP location can themselves be encrypted.

VPN

A virtual private network (VPN) adds security and privacy to networks and are usually used to protect sensitive data. For added protection, the hosting environment can also be configured so that the SFTP site is only accessible to remote clients that are connected to a VPN. Either the VPN would be hosted within the hosting environment or, alternatively, an existing VPN could be leveraged.



Part 3
Penetration testing

OVERVIEW

This section describes the various types of testing that Enable consistently performs to ensure that our clients receive the highest standard of software in terms of quality and security. By acknowledging the importance of infrastructure penetration testing and making it one of the vital steps in the implementation process, our software is more efficient and error-free.

PURPOSE

Web applications have become common targets for attackers as they can leverage relatively simple vulnerabilities to gain access to confidential information or even gain full control of the targeted environment. While traditional firewalls and other network security controls are an important layer of any information security program, they can't defend or alert against many of the attack vectors specific to web applications. It is therefore critical for Enable to ensure that its web applications are not susceptible to common types of attack.

The objectives of a penetration testing exercise would typically include:

— To identify any weaknesses that may be present, which an attacker aiming to compromise the confidentiality, integrity or availability of the client's systems and data could exploit;

— To identify the threats facing the client's information assets so that the level of risk can be quantified and addressed.

— To provide independent verification on the security risks of the target infrastructure and applications to ensure that the client's security expectations and requirements are being met;

— To provide the client with assurance that a thorough and comprehensive penetration test covering policy, procedure, design and implementation has occurred;

— To adopt best practice by conforming to legal and industry regulations;

— To ensure protection against common types of attacks like cross-site request forgery (CSRF), cross-site scripting (XSS), path traversal and SQL injection.

THIRD-PARTY TESTING

In the event of penetration testing being organised by the client, Enable will liaise with the client, the testing company and the hosting provider to ensure that the test takes place smoothly. Enable's clients frequently request that external penetration testing is carried out by a third-party security company and these tests cover both the software application and the hosting infrastructure to ensure that correct configuration and recommended practices have been followed to minimise client exposure.

The services performed when carrying out an application test vary according to the risk category of the site and the technology and protocols that have been implemented. Many companies have adopted the Common Vulnerability Scoring System which is designed to convey vulnerability severity and help determine urgency and priority of response.

Enable has passed all 14 of these tests that it has taken over the last five years. Should any penetration test issues arise these will be managed via Enable's standard non-conformance procedure.

Managing security breaches and attacks

OVERVIEW

Enable has a tried and tested incident management plan to respond to any security breaches and attacks. A fast response and strict compliance to these procedures can prevent unnecessary harm coming to our infrastructure and minimise the potential for stolen sensitive data falling into the wrong hands.

MANAGEMENT OF SECURITY INCIDENTS

Upon the discovery of a security breach or attack, Enable will take measures to stop it with immediate effect and investigate how it occurred and what measures can be taken to prevent such a breach from happening again.

The steps taken will depend on the nature of the incident but may include stopping and disabling affected services or minimising or removing methods of accessing a server via applicable network protocols. All available applicable logs — which may include security logs, firewall logs, IDS logs, IIS logs, SQL Server logs, antivirus logs, and logs from monitoring services — will be checked for information pertaining to the breach.

Enable will also investigate the state of any affected servers, their applications and data in order to assess any impact as a result of the security breach or attack. Using evidence gathered at this stage will allow us to take any necessary remedial actions in addition to the preventative measures that are covered below.

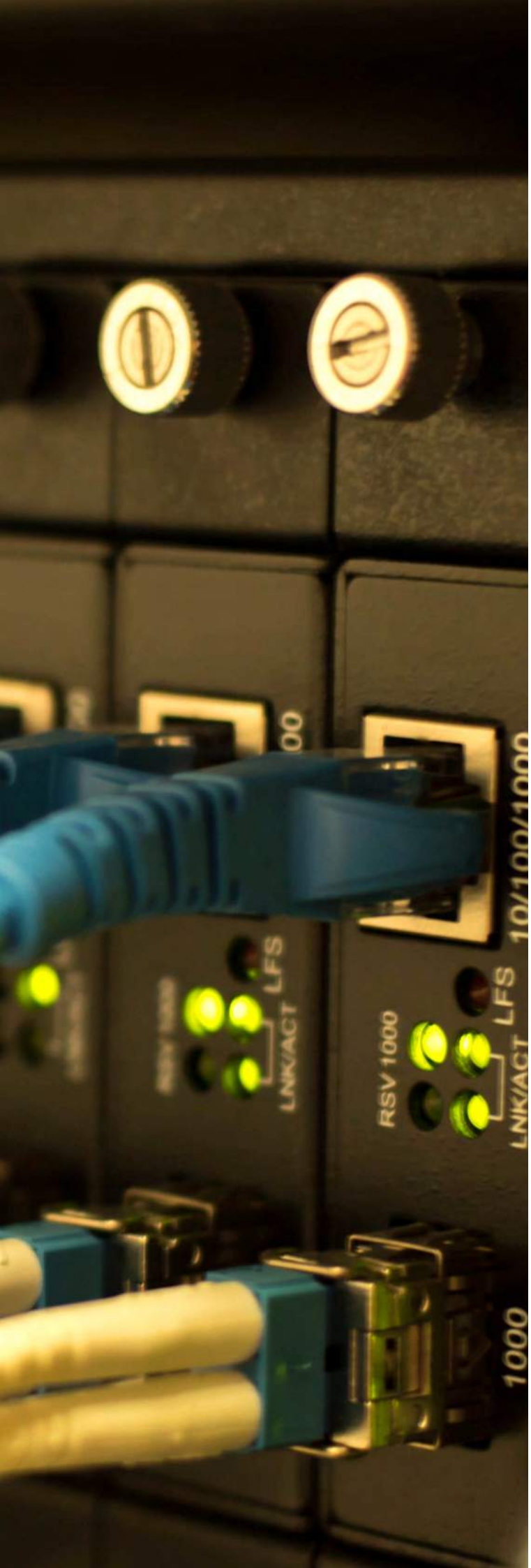
When the nature of the breach is understood, measures are taken to prevent it from happening again including changes to firewall configuration, changes to server configuration and applying system and/or software patches, updates or firmware upgrades to network infrastructure devices.

Enable will always disclose any security breaches or attacks to the client from the Enable Helpdesk. This will include a report with information from the preventative actions, investigation, remedial actions and improvements resulting from the steps mentioned above.

THREAT MANAGEMENT, MONITORING CONTROLS AND INCIDENT DETECTION

Server security and antivirus logs are manually reviewed on a weekly basis with any anomalies uncovered followed up as a priority in order to mitigate any risks. In the event of a security incident, Enable will take measures to stop it with immediate effect and then begin an investigation into the source and identify measures to be taken to prevent such an attack from happening again.

Archive logs and backups can be retrieved to check for misuse of data, such as unauthorised access. During the course of an investigation following a security breach or attack, all available applicable logs will be



checked for information pertaining to the incident with logs that are applicable dependent on the nature of the incident.

SECURITY MEASURES

Enable has a number of security measures in place to prevent and resolve security breaches or attacks. These include hardware and software firewalls, antivirus software, regular operating system updates, software updates and email filtering.

It is company policy that all workstations and servers are covered by approved antivirus software – which in the case of Enable means a combination of Symantec Endpoint Protection and Sophos.

In addition, the Enable network is protected by a perimeter hardware firewall and, internally, each server and workstation is configured to run Windows Firewall without exception. The configuration for servers and workstations is distinct and controlled via separate Group Policy Objects (GPO) in Active Directory (AD). The servers in the production environment are protected by a Cisco ASA 5510 Sec+ firewall.

Throughout the organisation, firewalls are also configured to only allow access through the ports that are absolutely necessary for a server or workstation and only allow access to authorised IP addresses.

Firewalls undergo a review on a quarterly basis to ensure that their configuration is up to date and as secure as possible while all emails sent and received by Enable are filtered by FuseMail — this protects Enable from spam and potential viruses or infections. Enable staff also check for operating system updates on a weekly basis and these are only applied once they have been manually approved by the IT team.

Updates to other pieces of software are reviewed on a monthly basis and their application to Enable servers is only undertaken once they have undergone proper planning.

Disaster recovery plan

Part 1
Approach

As a company whose primary products are internet based applications, it is of paramount importance to Enable that our ability to host our clients' applications remains unaffected in any eventuality as far as can be reasonably expected. Enable has a thorough disaster recovery plan which is tested twice a year, then thoroughly reviewed before being used as a basis to continually improve the disaster recovery plan and ensure Enable staff are best placed to respond to a disaster recovery scenario.

PROCESS

Should our disaster recovery plan need to be activated, Enable will inform the primary contact of any affected clients of the situation and log the issue on the Enable Helpdesk as a category A ticket.

Enable will then contact the client regularly to provide them with updates on the status of the disaster recovery process and immediately inform them once their system is back online and operating normally.
The first point of contact at Enable when a system becomes unavailable is the Enable Helpdesk.

PREVENTATIVE MEASURES

A number of preventative measures are in place to ensure the secure running of the Enable production environment.

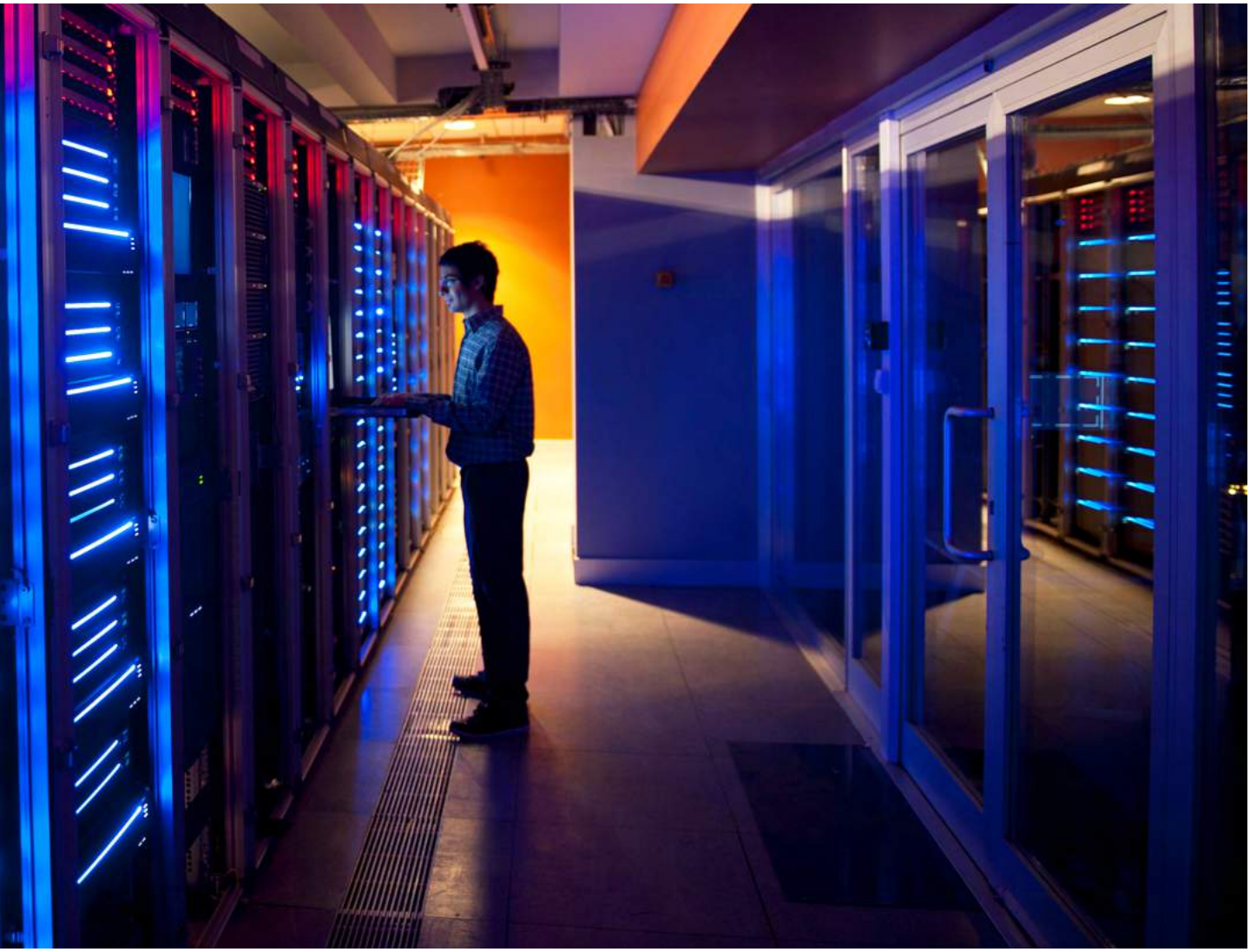
All Enable production servers are monitored by independent systems from both Enable and the host. Both systems raise automatic alerts via email in the event that a server experiences an outage.

Enable has a tiered approach to application and server backups, as discussed on page 8. Enable will ensure that its disaster recovery and resilience arrangements:

— Provide for backups of customer data and the retention of not less than 30 days of onsite backups;
— Permit data to be replicated to an alternate site using a secure high-speed private fibre network;
— Provide for compliance with time limits for RPO and RTO.

CLOUD SERVERS

Cloud servers offer resilience, flexibility and recoverability advantages over traditional dedicated physical servers. Due to the nature of cloud servers, where the whole server is abstracted from specific computer hardware, the risk of a single piece of



hardware failure affecting a server is greatly reduced.

In the event that a cloud server does go down, the first step is to open a dialogue with the host and rule out a possible server hardware, network or power failure. If the cloud server has gone down due to a problem not covered in the above list, a new cloud server will be created using the most recent full image backup available and, in any case, a full investigation will be undertaken in order to identify the cause of the server outage and to plan follow-on remedial action. In the event that there is a fundamental issue with the host's cloud solution, steps will be taken to redeploy affected systems to suitable alternative hosting.

DATABASE RECOVERY

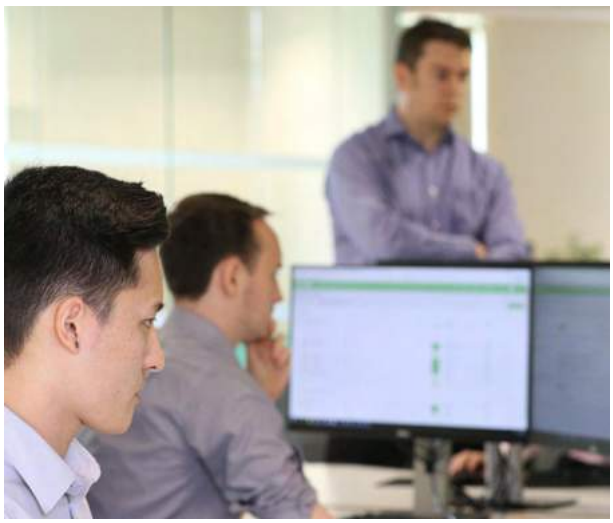
In the event that a disaster recovery scenario requires the restoration of application databases, the most recent full database backup and applicable transaction log backups will be restored to a replacement or alternative hosting environment.

POWER SYSTEM / NETWORK

The host implements an N+1 redundancy policy on their power systems and network routing and, for the power systems, there are also dual incoming utility feeds from separate substations off two isolated grids. The host guarantees that their data centre network will be available with the data centre HVAC and power functioning 100% of the time in a given month, excluding maintenance.

IMPLICATIONS TO URL OR DNS CHANGES

In the event that the disaster recovery procedure results in alternative hosting, such as a new physical or cloud server, then it is likely that the IP address of the new hosting environment will differ to that of the previous hosting environment. Where Enable has administrative control over the relevant internet domains, Enable will make the necessary DNS updates. Where Enable does not have administrative control over affected internet domains, we will communicate the necessary DNS changes to the client's primary contact.



Part 2
RPO and RTO

A recovery point objective (RPO) is defined by business continuity planning and is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity.
In simpler terms:

— RPO stands for how recently it will be able to recover to in the event of a major incident

— RTO stands for how quickly it will be able to recover from a major incident

Enable understands that having a robust disaster recovery plan in place and conducting regular disaster recovery plan testing is a part of establishing RPOs and RTOs and we work with clients to design infrastructure to meet their RPO and RTO requirements.

As an example, Enable is able to achieve an RPO of four hours and an RTO of eight hours, with the qualification that the scope of the RPO and RTO is set for a single geographic site.

R P O

To provide an RPO of four hours, Enable takes regular database transaction log backups in addition to daily full database backups. Our standard transaction log backup schedule in the production environment is to do this every four hours. With this in place, given a scenario where database data needs to be recovered, Enable will restore the application data to a state that it was in — to a point in time that is at most four hours prior to when the data was removed, updated or corrupted. The integrity of the transaction log backups is verified automatically as part of the backup process.

R T O

To provide an RTO of eight hours, Enable uses the services and data centre provided by the host, which are solely run and operated by the host alone.

The host guarantees that their data centre network will be available 100% of the time in a given month, excluding maintenance. The data centre network refers to the portion of the host network extending from, but not including, the outbound port on the cabinet switch to the outbound port on the border router. This includes the host's managed switches, routers and wiring.

The host guarantees that data centre HVAC and power will be functioning 100% of the time in a given month, excluding maintenance. Power includes UPSs (uninterruptible power supplies), PDUs (power distribution units) and cabling, but does not include the power supplies on servers.

Contingencies built into the hosting infrastructure design of the application include:

— Two load balanced web servers;
— Potential option of two clustered database servers, although this is out of scope for the initial hosting deployment;
— Application and database storage provided by shared storage area networks (SAN) storage;
— RAID arrays used for local server storage and SAN storage;
— Potential for a redundant firewall to be included in the hosting infrastructure design.

Therefore, with regard to the failure of a single piece of hardware in the hosting infrastructure design, there are partner devices that can assume a given role on a temporary basis should a device require a repair or replacement.

Regarding hardware faults requiring repair and replacement, the host guarantees the functioning of the following provided hardware:

— Switches, firewalls, load balancers and servers;
— Direct attached storage devices;
— Network attached storage devices;
— SAN.

Hardware repair or replacement will begin once the host identifies the cause of the problem and is guaranteed to be complete within one hour of problem identification for switches, firewalls, load balancers, servers and direct attached storage devices.

For SAN hardware failures, we guarantee that we will have a technical specialist and necessary parts onsite to begin repairs within four hours of problem identification.

The hardware guarantee excludes the time required to rebuild the system, such as the time required to configure a replacement device, rebuild a RAID array, reconfigure devices from their default settings, reload operating systems, reload and configure applications and/or restore from a backup.

FIND US ONLINE

ENABLE.COM

HELLO@ENABLE.COM

UK OFFICE

+44 203 998 7470

10-12 THE COURTYARD
STRATFORD-UPON-AVON
CV37 9NP, UK

USA OFFICE

+1 628 251 1057

535 MISSION STREET
14TH FLOOR, SAN FRANCISCO
CA 94105, UNITED STATES