People

SECURITY MANAGEMENT

HOW WE PROTECT YOUR SENSITIVE DATA

www.peoplehr.com | security.peoplehr.com

An Introduction from our MD and CTO

Sat Sindhar, Managing Director

"Here at People® we take security very seriously. We know how important data security is to our customers, and want you to feel comfortable in the knowledge that your data is in very safe hands. We designed this guide to show you how we manage and maintain our security processes. Please do contact us if you have any questions about the information in this guide, we'd be happy to answer them for you."

Sukhjinder Singh, Chief Technology Officer

"My background in IT extends over 25 years, mostly working for an Investment Bank. I have been working with People® since the company began, and I was involved in the initial development of the system. I have since moved onto looking after our information security which has included the implementation of our ISO27001 Information Security Management System, and am proud to present to you how we manage information security here at People®.

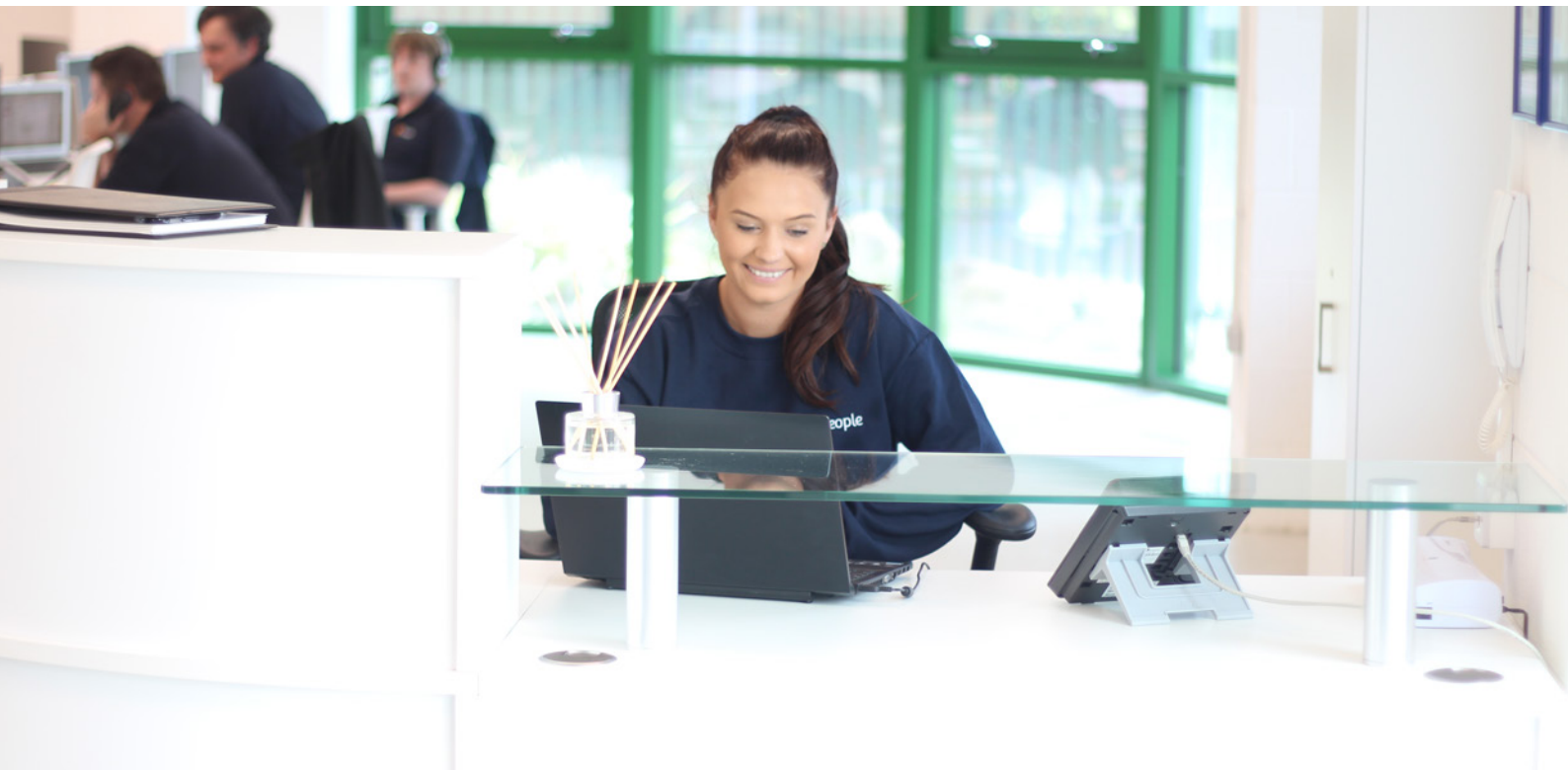


Table of Contents

Keeping Your System Safely Online

The Data Protection Act, 1998 requires every data controller who is processing personal information to be registered with the Information Commissioner's Office (ICO). People is registered and our registration number is ZA185401.

Our Information Security team is responsible for ensuring our information security policies are compliant, and properly implemented. They also handle many of the information security questions raised by our clients.

We are ISO27001 accredited, our data controller is ICO registered, and we also source third party penetration tests.

The most significant service issue is unexpected downtime. We monitor our systems around the clock, including weekends and public holidays. This means that should a critical error occur, we are instantly notified, and can immediately react.

- Throughout 2017 our system has been available to customers for an average of 99.9% of the time.
- Our average response to system downtime took 677 milliseconds. You can verify these statistics at:

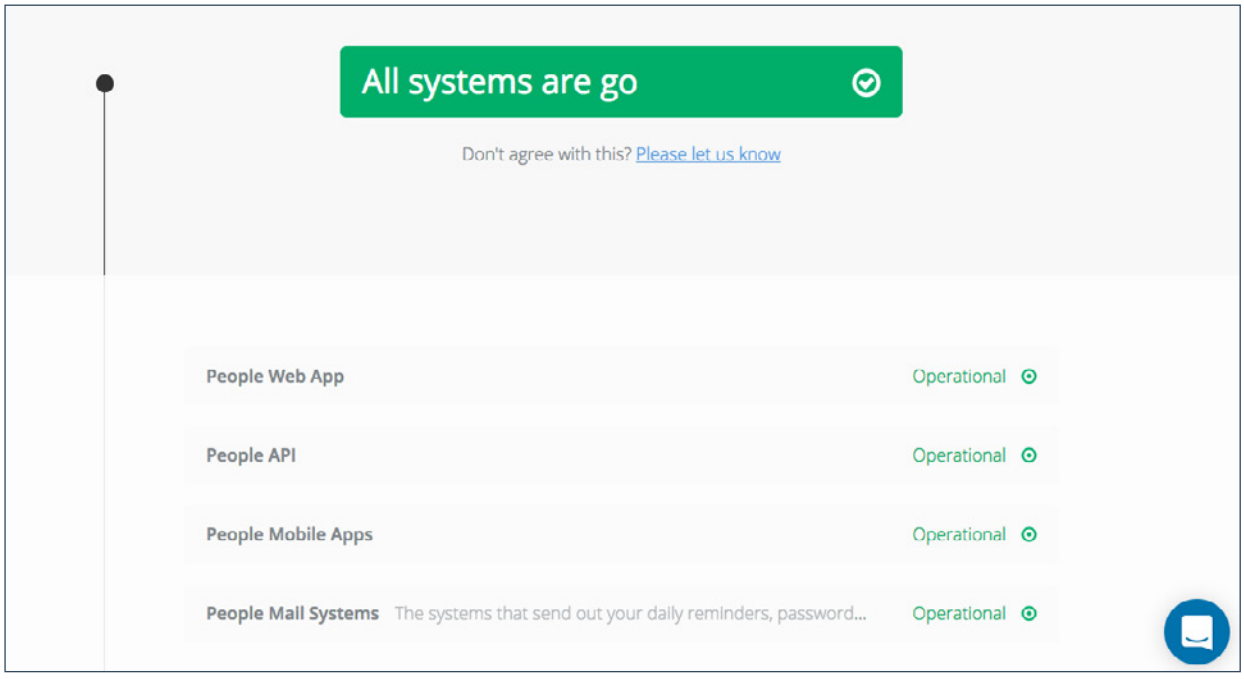
http://bit.ly/2Cid10j

In the event of an infrastructure issue that cannot be fixed, we will implement our disaster recovery plan. This will allow us to fully restore People onto an alternative infrastructure. No customer data will be lost.

The People infrastructure is highly resilient. Even in the event of a load balancer, firewall, a web server or a sql server failure, the service will automatically switch to alternative devices and you will not be impacted. Again, no data will be lost. However, should a critical issue result in system downtime, then our immediate priority becomes resuming normal service.

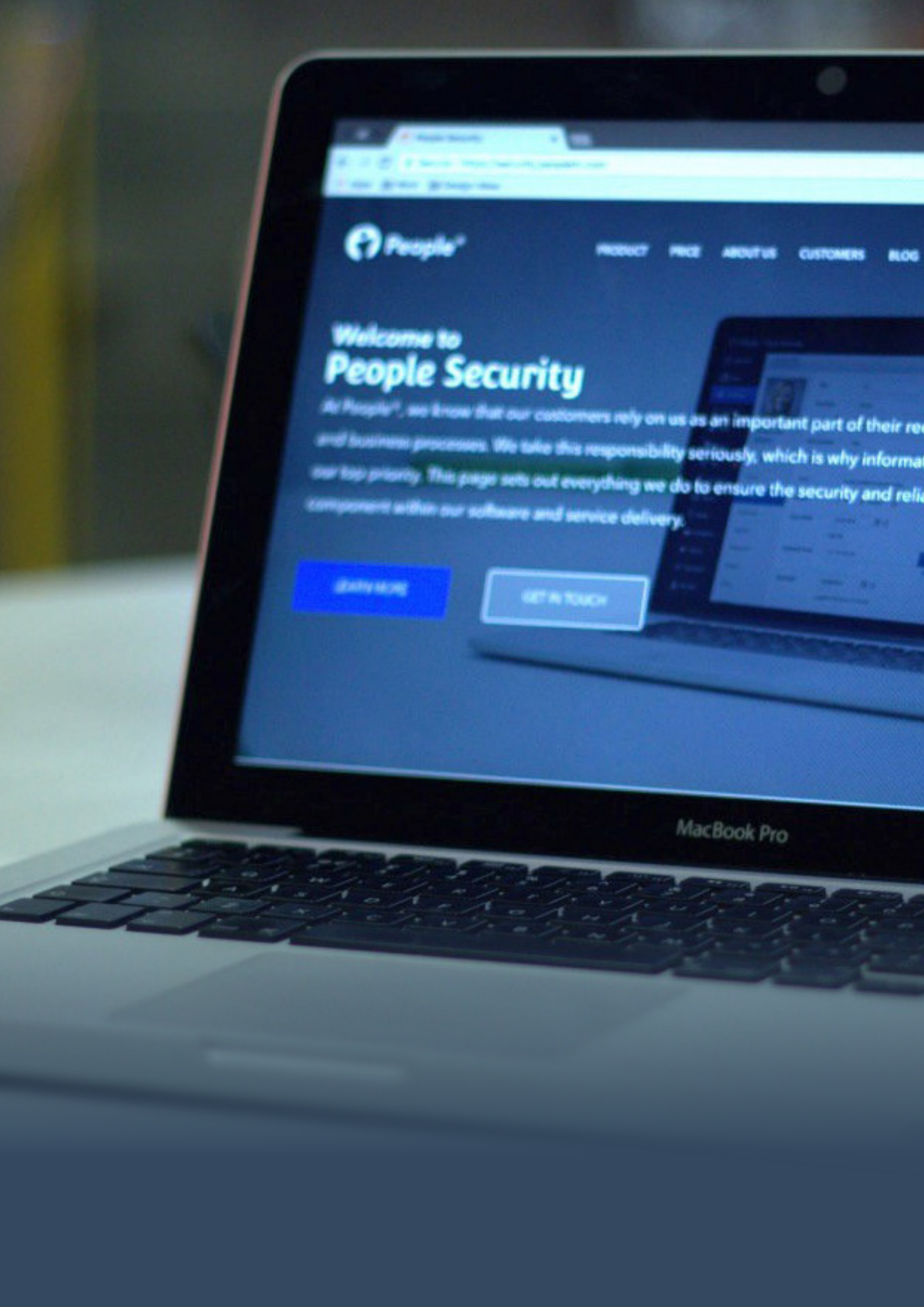
During this time, here are the steps we follow:

- We will provide you with a status alert. If our system is down, we will update our status page to ensure all customers are aware. You can check our status page here at any time: **http://status.peoplehr.com** — you can enter your email address to be instantly alerted whenever the status changes.



- We will give you an issue overview. When our system status changes, we will provide as much detail as we are able, in terms of who the issue is impacting, which areas of the system are affected, and an estimate of when service delivery will return to normal.

- We will keep you updated regularly. Following our initial status alert, we will provide 30-minute updates whilst working to resolve the issue, until service delivery returns to normal.


PRODUCT
PRICE
ABOUT US
CUSTOMERS
BLOG
Welcome to
People Security
MacBook Pro

Information Security FAQ's

Who owns the data?

- Your data belongs to you. As our customer, you are classed as the 'data controller'. As your supplier, we are classed as the 'data processor'.

What happens to our data when we leave?

- We provide you, the customer, with an export of all your data, and then remove it from our systems within 45 days. Any documents you uploaded will be returned in their original format. Anything else is sent in CSV format.

How often is our data backed up?

- Your data is backed up per transaction (each time you do something), per hour, and per night, and the data is stored for two weeks. In the event of a total failure, our infrastructure within the data centre means we can recover your data quickly and reliably. If you have particular governance rules, you may also create your own backups using our offline backup tool.

Where is our data stored – and is it safe?

- We store your data in Rackspace's state-of-the-art data centre in London, UK. Rackspace protects the servers where your data is stored and managed, through biometric access controls, constant surveillance, redundant power feeds and generators, robust fire suppression, and carefully monitored climate control. In keeping with Data Protection Act requirements, we guarantee that your data will never be moved outside of the EEA (European Economic Area). Your data is also encrypted using TLS (Transport Layer Security) and AES (Advanced Encryption Standard).

Who can access my data?

- Only you, and a small number of vetted and authorised People personnel, can access your data. Any member of this specialist People team, will only ever access your data to perform specific tasks on your request via our support desk – and any action they take is logged and easily audited. Access to any sensitive data is extensively logged, and requires fixed IP addresses and two-factor authentication.

What type of Firewalls do you use?

- The People application, and any data you store within it, is protected by Ciscopowered firewalls

Offline Security Measures

We have offline processes in place for reporting any potential security threats to our system so they can be assessed and removed if necessary.

Here are the security practices we follow in our offices to ensure the safety of customer data:

- Equipment stored in lockers when not in use
- Screens are locked when an employee is not using them
- Paper based information is shredded as soon as it has served its purpose
- We take care not to leave printed information in holding trays for any undue amount of time, and always make sure to send documents to the correct printer
- Employees who handle sensitive data have privacy screens so only they can see what they're working on
- Desks are cleared at the end of the day so that breaches don't occur when the office is out of hours

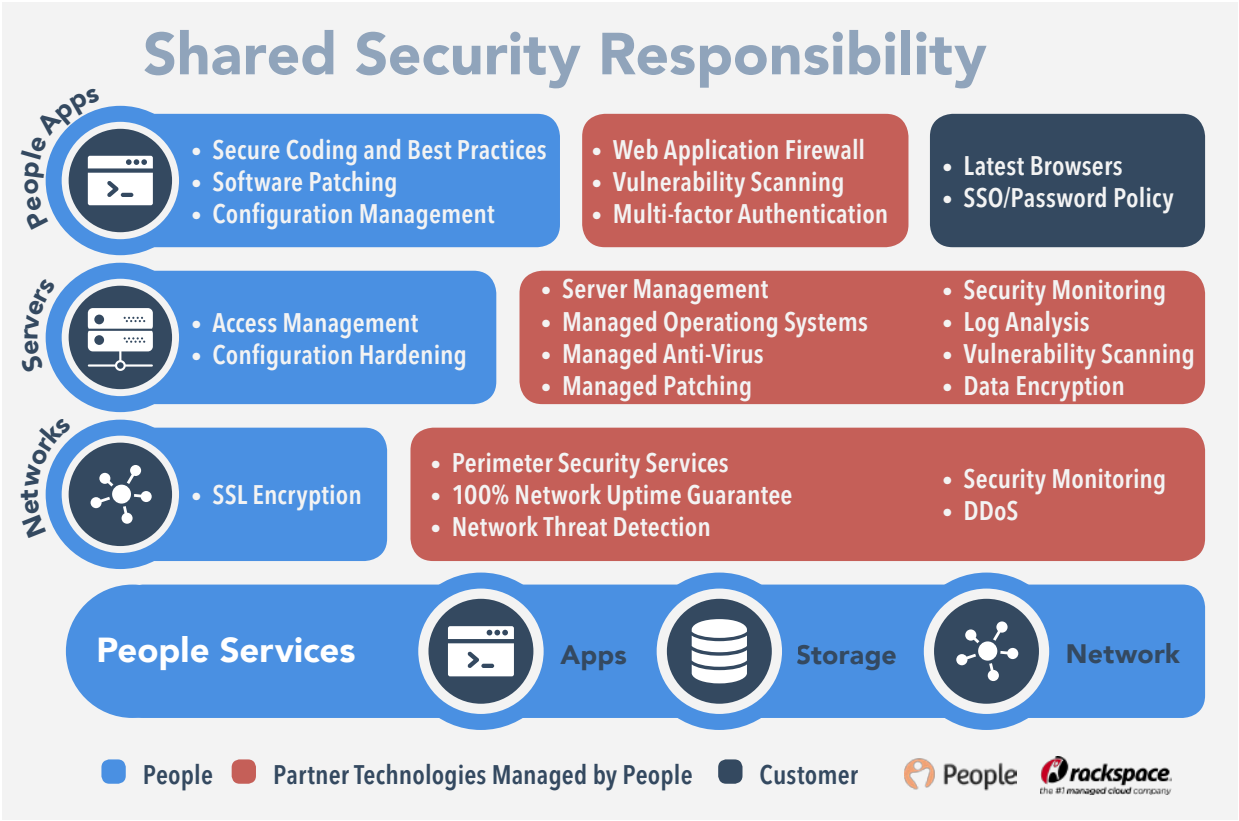
ISO27001 Accreditation

This accreditation is the international standard for information security. In order to be accredited by the International Organization for Standardization (ISO), we had to implement several controls for a best practice information security management system. This included assessing our practices; we took the following actions:

- Updated our information security policy, and implemented strict controls for our employees in regard to the access and use of company premises and equipment.
- Identified legal, regulatory, contractual and other requirements for an information security management system.
- Conducted extensive risk assessments and identified risk treatments
- Formulated training and awareness plans
- Prepared internal audit procedures
- Conducted management reviews
- Conceived forms, and procedures for corrective action

Technical Information

The following diagram displays how we manage data security across our application, servers and our network. The blue boxes toward the left, and the bottom of the diagram below represent responsibilities that People take care of. Red boxes detail the responsibilities Rackspace look after on behalf of People and the customer. The customers only responsibilities when utilising People's services, are to make sure their browsers are up to date and that they implement a secure SSO/Password policy.



Actively searching for threats is important for keeping your business safe. That's why we work with Rackspace, through their Managed Security Service.

People

Our environment is looked after by a 24x7x365 Customer Security Operations Center (CSOC), staffed by best-in-breed, GIAC certified intrusion analyst (GCIA) and GIAC certified intrusion handler (GCIH) certified security analysts, whose credentials meet or surpass industry standards.

Process

Using Rackspace Managed Security (RMS) means we don't just detect threats, but we also rapidly respond to them - performing appropriate remediation based on preapproved actions.

Technology

Our partnership with Rackspace means we actively counteract threat activity through industry-leading host and network protection, threat intelligence and security analytics, log management and vulnerability management technologies.

https://www.rackspace.com/resources/managed-security-services-overview

Managed Security provides active threat detection and remediation for cyber-attacks. Whereas most managed security service providers only notify customers about a breach, leaving it to the customer to respond, Rackspace Managed Security (RMS) utilizes preapproved actions to immediately remediate security issues.

RMS service Includes:

Configuration hardening and monitoring:
Detects and logs deviations from assigned security configuration profiles in real-time to allow for comprehensive documentation and reduced vulnerability windows.

Patch monitoring:
Provides an understanding of any threats that are applicable to an environment including which common vulnerabilities are present in the environment.

User monitoring:
Monitors and documents user host access, authentication levels and login times to ensure that customers can prove compliance with access controls.

File integrity management:
Detects, reports and documents changes to files on a host based on our security and compliance requirements.

Host-based protection:
Real-time visibility into adversary activity on every endpoint. Analyses billions of endpoint events, spotting and correlating anomalies to alert us when an attack is underway.

Net-based protection:
Intrusion detection to increase the security level of networks, monitoring traffic and inspecting and scanning packets for suspicious data.

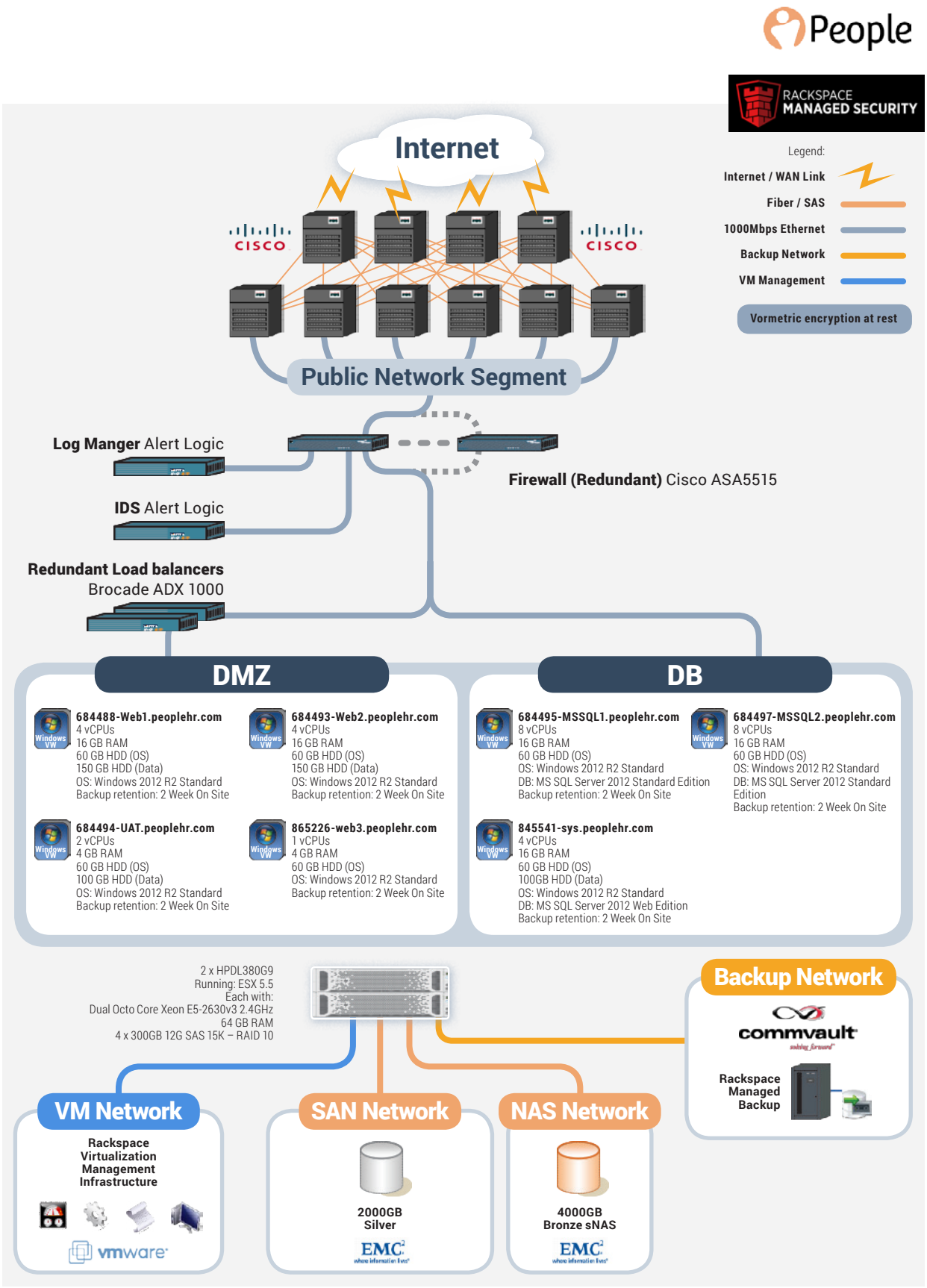
Security analytics:
Advanced technologies augmented by behavioural analytics that enable the security team to aggregate, correlate, analyse and respond to security threats in the environment.

Log Manager:
Collects, aggregates and normalizes log data which is then analysed by the security team.

Web Application Firewall:
Protects against web application threats such as what is covered in Open Web Application Security Project (OWASP). These include threats such as SQL injections and cross-site scripting.

DUO Security –
Two Factor Authentication:
Two factor authentication enables an additional validation to users trying to login via RDP or SSL VPN. This ensures anyone accessing the database (for example) definitely has the authority to do so. This prevents unwanted users stealing admin usernames and passwords to access our data/ application.

System Architecture



Firewall: *Two Cisco ASA5515's:* these support antivirus, malware protection, remote access authorisation, access control, deep inspection and intrusion prevention.

Log manager: *Alert logic:* Real time log management and collection gives us increased visibility of security threats, allowing us to turn data into action to prevent breaches.

IDS (Intrusion Detection System): *Alert logic:* The intrusion detection system gives us the ability to spot threats before they are able to gain access to our system so they can be dealt with.

Load balancers: *Two Brocade ADX 1000's:* These ensure the use of our resources are optimized without breaching any service level agreements.

DMZ (Demilitarized Zone): This area contains four virtual machines which allow access to untrusted networks (such as the internet). This effectively means it acts as a buffer to the Database server.

DB (Database): The database server has three virtual machines with a thicker security layer than the DMZ. The data is held over two virtual machines and a copy of the data is held on the third virtual machine.

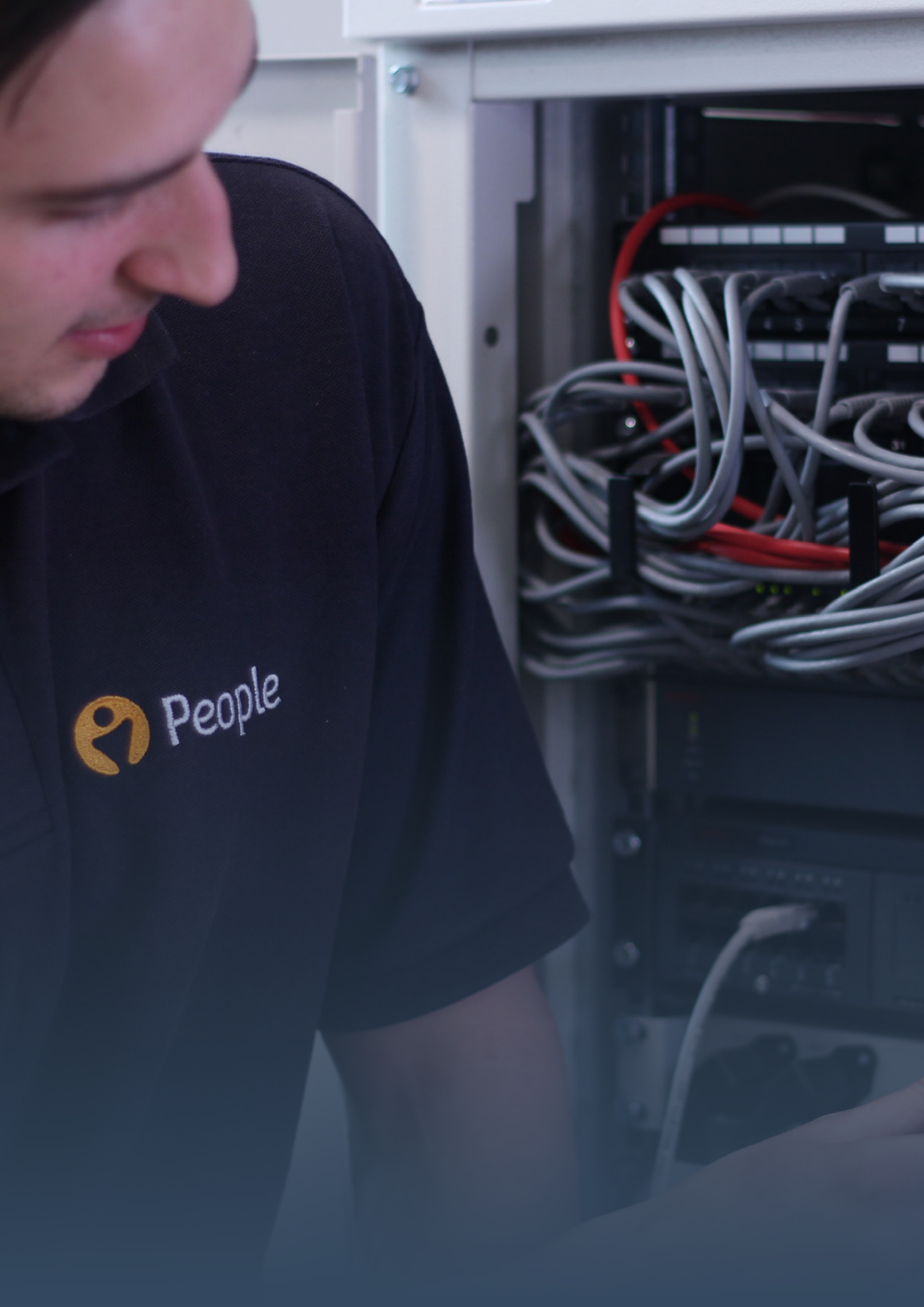
VM Network: Two hypervisors host and manage the virtual machines on our network.

Backup: All of our virtual machines and storage are backed up daily. Our database is backed up every 15 minutes. A copy of all data is retained for two weeks.

SAN (Silver): Storage Area Network gives a high-speed network of 2TB storage devices available to applications running on the networked servers. Silver provides faster access to files than bronze, the database is stored here.

SAN (Bronze): Storage Area Network gives a high-speed network of 4TB storage devices available to applications running on the networked servers.

Vormetric encryption: Easy to deploy cloud encryption, that maintains control of data. This type of encryption means that our system protects your data at rest. This eliminates malware threats and renders stolen data useless to hackers, as they will be unable to see any plain text or documents, such as payslips or employment contracts. Vormetric encryption uses a key management system, and continuously collects security intelligence in order to monitor access to data. Vormetric encryption satisfies article 25 of the GDPR which suggests that a company should have "Data protection by design and default".


People

Disaster Recovery Plan

We have a full disaster recovery plan (DRP), that will be followed when a disaster arises. This chapter is a brief overview of what the plan entails.

Purpose

In the event of a disaster the first priority of People is to prevent the loss of life. Before any secondary measures are undertaken, People will ensure that all employees, and any other individuals on the organisation's premises, are safe and secure.

After all individuals have been brought to safety, the next goal of People will be to enact the steps outlined in the DRP to bring the facility back to business-as-usual as quickly as possible. This includes:

- Minimising downtime to the facility
- Preventing loss to customer data

Definition of a Disaster

A disaster can be caused by man or nature and results in the facility not being available for a period of time. People defines disasters as the following:

- A failure in the data centre that results in the facility not being available to a significant number or all users
- One or more vital components of the facility not being available
- Loss of any client data

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- Outage at the data centre
- Failure of key infrastructure at the data centre

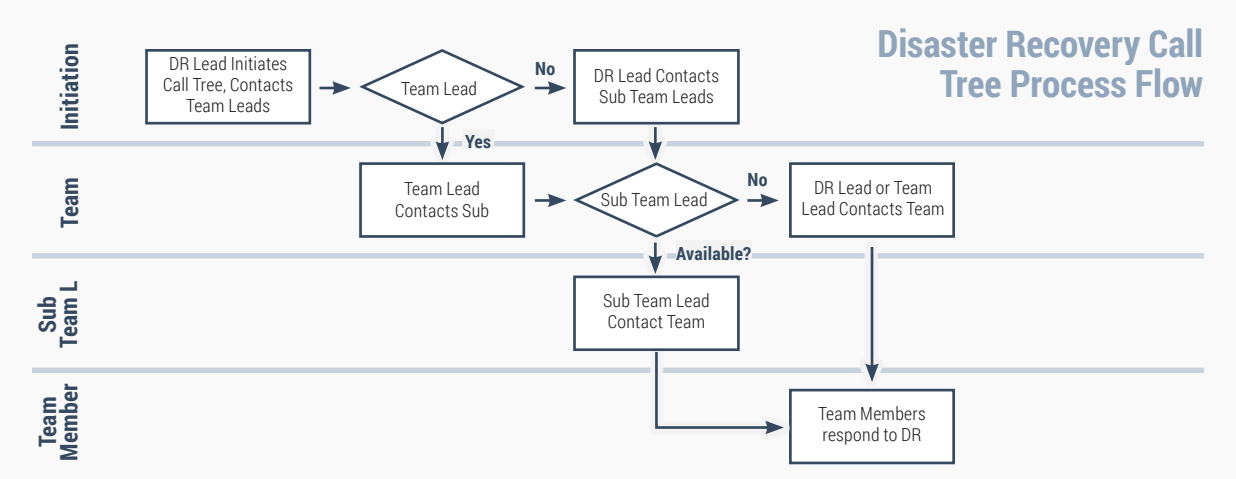
Dealing with a Disaster

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

1) Disaster identification and declaration
2) DRP activation
3) Communicating the disaster
4) Assessment of current and prevention of further damage
5) Standby facility activation
6) Establish operations
7) Repair and rebuilding of primary facility

Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so People will make use of a call tree to ensure that appropriate individuals are contacted in a timely manner.



Communicating During a Disaster

The Communications Team's first priority will be to ensure that the appropriate authorities have been notified of the disaster.

The Communications Team's second priority will be to ensure that the entire company has been notified of the disaster.

After all of the organisation's employees have been informed of the disaster, the Communications Team will be responsible for informing clients of the disaster and the impact that it will have on the following:

- Anticipated impact on service offerings
- Anticipated impact on delivery schedules
- Anticipated impact on security of client information
- Anticipated timelines

Communicating with Vendors

After all of the organisation's employees have been informed of the disaster, the Communications Team will be responsible for informing vendors of the disaster and the impact that it will have on the following:

- Adjustments to service requirements
- Adjustments to delivery locations
- Adjustments to contact information
- Anticipated timelines

Plan Testing & Maintenance

While efforts will be made initially to construct the DRP as complete and accurate as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors the DRP plan will be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

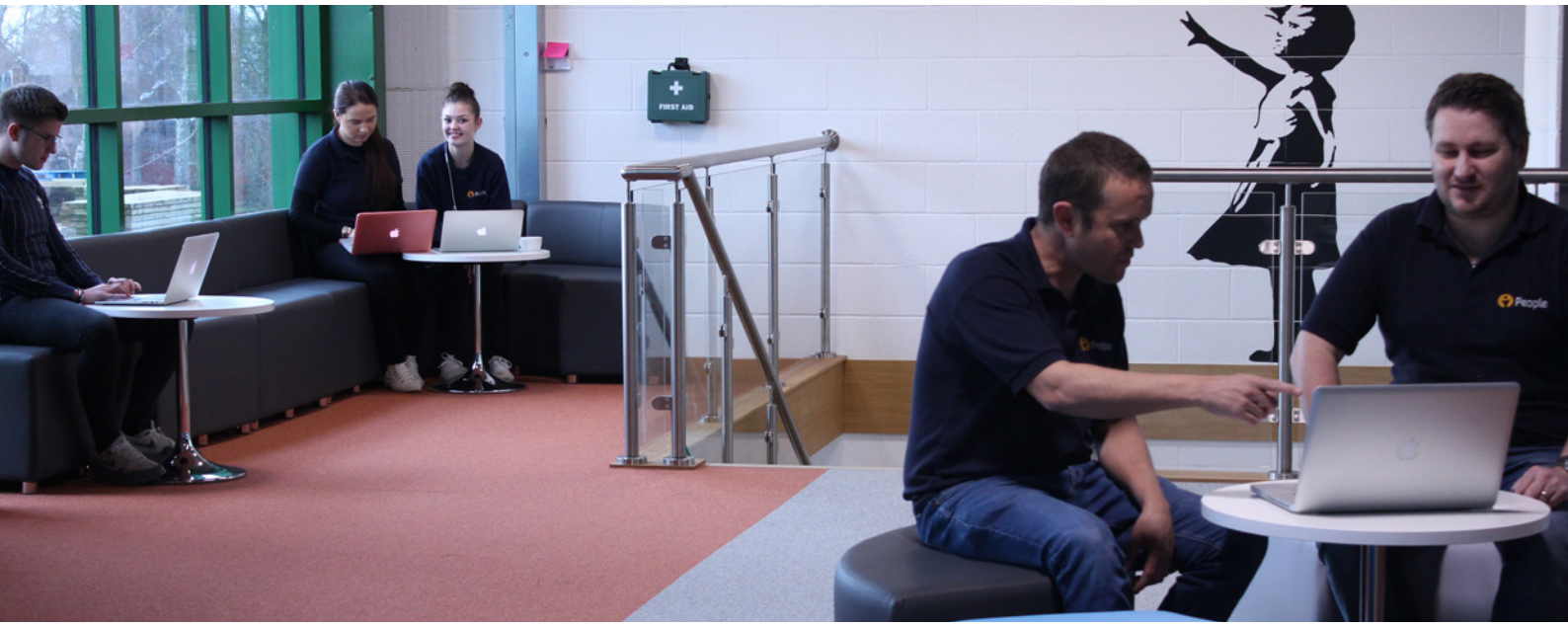
Maintenance

The DRP is updated every six months or any time a major system update or upgrade is performed, whichever is more often.

Testing

We are committed to ensuring that this DRP is functional. The DRP is tested every six months in order to ensure that it is still effective.

About People



People HR is a human resources management system, used by thousands of progressive HR professionals who want to make better decisions, fully engage their workforce, and deliver high-impact results that influence their organisation's success.

Beyond helping you migrate from spreadsheets, paper files and repetitive tasks, People HR helps you make your work more meaningful. In-built advice based on HR best-practice guides your processes, while heatmaps, alerts and reminders inform your decisions and keep you in top form.

Visual, clutter-free, and easy to pick up, People HR does not ask you to re-learn your job. Instead, it focuses your attention on the tasks that will make the biggest difference, to help you grow your business and master your career.

Modern and web-based, People HR is developed by a team of HR experts who are always finding new ways to keep you three steps ahead. Employees and managers alike will find it easy to manage their own routine tasks from anywhere in the world, and you'll make a big impression at every level of business – from giving front-line employees a holiday booking system that makes sense, to showing your board-level directors the impact HR has on their bottom line.

This document is provided as a general guide. It is not legal advice, or an instruction manual. Features and/or benefits depend on system configuration and are subject to change, without notice. People® cannot guarantee the accuracy of any information presented, after the date of publication. Your implementation of the measures described may not result in your compliance with law, or other standard. You should not rely solely on this document to decide whether or not to purchase the service.

People disclaims any representation, express or implied warranties, including any implied warranty of merchantability, fitness for a particular purpose, and non-infringement, or other legal commitment regarding its services except for those expressly stated in a People services agreement. Other People or third-party trademarks, service marks, images, products and brands remain the sole property of their respective holders and do not imply endorsement or sponsorship.

Thank you for reviewing our security management

People