Service Infrastructure, Security and Disaster Recovery

The goal of the e-permits SaaS (Software as a Service) application is to provide the best in class work access and permit to work solution through the use of secure, high performance infrastructure that is highly available.

This document summarises the infrastructure, security provisions and disaster recovery in place to ensure this is achieved.

Service Provider

The e-permits application is hosted by IOMART plc (https://iomart.com), between two, tier three, UK based datacentres that offer 99.995% uptime. IOMART have many accreditations including: ISO 27001:2013, ISO9001:2008, ISO 14001:2004, ISO 20000, ISO 27018:2014, ISO 22301:2012, OHSAS 18001:2007, ISO 17788:2014, ISO 17789:2014 and SSAE 16 SOC1 & SOC2. See https://www.iomart.com/about-iomart/accreditations/ for more details.

Support is available 24x7 through onsite network operations centre and technical engineers. The network is secured by intrusion prevention systems, diverse fibre routing via multiple carriers and redundant cross connectivity to multiple tier 1 carriers ensure high performance and high availability. You can read more here: https://www.iomart.com/about-iomart/uk-data-centres/

Service Infrastructure

The infrastructure designed for the e-permits solution includes dedicated redundant firewalls, web application servers and database servers. Servers and firewalls are configured using hardened and patched operating systems with RSA secured VPN and Access controls to prevent unauthorised access. All access is recorded via independent logging software to ensure a full audit trail is maintained.

Banyard Solutions Limited
T: +44 (0)1483 413770
www.banyardsolutions.co.uk

Security

Network security threats from Internet-born worms and viruses, internal data loss, natural disasters and terror related incidents pose a serious threat to any organisation storing data electronically.

We take these threats very seriously: the security of sensitive company data is central to our approach and for this purpose we use the industry's most potent security tools and techniques, designed, built and maintained specifically for cloud based hosting.

Data is encrypted in transit and at rest to ensure at no point will your information be exposed to prying eyes.

Anti-virus, anti-malware and anti-spyware is installed on each server component. Data is both physically and logically separated for each customer and all ingress points are subject to intrusion detection and prevention systems. Formal patching of servers and appliances happens out of core hours on a monthly basis to ensure security standards are maintained.

Performance & Monitoring

Performance and availability monitoring is configured to alert IOMART and e-permits support staff of potential issues before they can become a threat.

Each part of the service infrastructure is monitored and can be scaled up to meet demand as the need increases.

You can view the public status of the e-permits application here: http://status.e-permits.co.uk

Disaster Recovery & High Availability

Each part of the e-permits service infrastructure is replicated in a hot DR site with automated failover at each layer including DNS failover, web application and database layer always on configuration.

We operate in a highly available environment; this is different to a disaster recovery model where, in the event of an outage, the entire infrastructure would have to be recreated to bring the service back online. High availability means each part of the service is synchronised with a replica and if one fails the system switches over to its counterpart.

IOMART maintain full onsite backups for 31 days for each web server and database server. We operate to an RTO (recovery time objective) of 1 hour (failover to the hot DR site can be dependent on DNS replication coming online) and an RPO (recovery point objective) of 24 hours (the time between backups).