Keeping Your Payroll Data Safe

Payroll Security

Computing Environment Protections

HRPro and our payroll partner, ECCA, recognizes the importance of system availability and the need to have the computing environment available and operating as designed. In the event of an unscheduled outage, we recognize the need to restore the computing capabilities as quickly as possible.
ECCA's data center is designed to provide high levels of service and redundancy for our client. Listed below are the key features of the data center and the service design.

Monitoring

System monitoring is used to proactively identify issues before they become service impacting problems. The goal is to reduce downtime and maintain performance. All aspects of the network – including associated hardware devices, servers and software applications - are monitored. Capacity thresholds are monitored, and engineers are notified when those thresholds are exceeded (e.g., disk space, CPU utilization, memory utilization, network bandwidth, etc.)

System Intrusion Defense

ECCA's system is protected by multiple layers of security including firewall appliances and intrusion detection software. All system are monitored around the clock to prevent the introduction of viruses and malware as well as systems that continuously scan for malicious or suspicious behavior on the network.

Electric Power

The data center is powered by the local electric utility. In the event of a power outage, all necessary equipment in the data center is backed-up with a battery-based uninterruptable power system (UPS). A natural gas-powered generator capable of powering the entire data center and all environmental systems backs-up the UPS.

Data Backup

All data stored on ECCA's servers are backed-up on a regular basis as defined in our backup schedule. At a minimum, all systems are backed-up daily after business hours.
Multi-level sequential backups are stored onsite on a separate storage device for immediate availability and access. Daily automated routines are executed to maintain redundant multiple backups of data to off-site cloud-based storage providers.

Keeping Your Payroll Data Safe

Payroll Security

Service Resiliency

Each service is designed using both hardware and software technologies that ensure the system can quickly, and often automatically, recover from common problems. ECCA's system utilizes redundant physical servers with automated failover and virtual servers to mitigate potential equipment failure and outages.

Internet Connectivity

ECCA's data center is connected to the Internet using two high-speed connections routed through two independent service providers. These connections are internally routed through fault tolerant switches and redundant firewalls to ensure maximum availability of the data center's connection to the Internet.

Physical Security

ECCA's office has a security system including smoke and fire protection. It is connected to a call center monitored 24 hours a day, seven days a week. Access to the server room is restricted to key personnel only; a key code is required to gain physical access to the server room.

Environmental

ECCA's data center is equipped with heating and air conditioning with excess capacity to account for system failures and extreme temperature variations. The monitoring system notifies ECCA's staff when an unacceptable temperature level is reached.

Physical Security

ECCA's office has a security system including smoke and fire protection. It is connected to a call center monitored 24 hours a day, seven days a week. Access to the server room is restricted to key personnel only; a key code is required to gain physical access to the server room.

Catastrophic Loss

ECCA's production environment extensively uses virtual servers and server replication. This enables the company to efficiently move a virtual server to a number of physical servers when necessary. In the event of a complete loss of a production server the system automatically fails over to the replicated server for uninterrupted continued operations. In the event of the loss of the replicated server, the effected applications would be moved to an alternative in-house, physical server. This process would take approximately two hours to complete. If there was a complete loss of ECCA's office or employees were unable to gain physical access to the facility, ECCA would initiate the process of moving production to its Alexandria, VA office. This move would be completed within 24 hours.

Keeping Your Payroll Data Safe

Payroll Security

System Security Measures

ECCA's processors have engaged with David J. Peck and Associates (DJPaA) to provide managed security services (MSS) and fill the role of Virtual Chief Information Security Officer (VCISO). The security services provided by DJPaA complements the existing security controls in place at ECCA's office.

ECCA's current security controls exceed industry standards. Unlike other organizations, if an incident should occur, they are equipped to quickly identify, contain and remediate the issue while ensuring the protection of all data. Additionally, with full packet and log capture, and forensic system snapshotting, ECCA is able to know what systems and data were affected and not just rely on confirmation of data leakage to alert clients.

Some of the Services Provided by DJPaA

- Virtual Chief Information Security Officer (VCISO)
- Incident Response Planning & Analysis Services
- Incident Response Testing & Capability Analysis Services
- Emergency Incident Response & Post-Incident Response Services
- Ongoing Information Security Risk Assessment
- Digital Forensics
- An ongoing risk assessment process that evaluates the environment and potential changes
- Technology implementation procedures that include appropriate controls
- Measurement and monitoring efforts that effectively identify ways to manage risk exposure

Managed Security Services

- Log management and correlation of at least one year of system logs.
- Capture, archive and display logs in a central location.
- Recreate events based on logged data.
- Alerting of certain events
- Vulnerability assessments conducted weekly as part of the vulnerability and change management program.
- Identify system misconfigurations.
- Identify missing system patches.
- Identify improperly configured web applications.
- Identify devices that are easily compromised.
- Validate appropriate patch management in place.
- Network Management/Intrusion Detection

1025 N. Campbell Road, Royal Oak, MI 48067 | hrpro.com | 248-543-2644 | Fax 248-543-2296 | newbiz@hrpro.com

Keeping Your Payroll Data Safe

Payroll Security

Managed Security Services Continued

- Network-based and host-based intrusion detection systems (NIDS and HIDS, respectively).
- Analyze all network communication to determine anomalies, threats or abuse.
- Full packet capture of communication to “replay” any event.
- Files transmitted can be automatically extracted and saved.
- Full network forensic capabilities.

Intelligence

- Know malicious IP addresses and hostnames for black and whitelisting on perimeter
- devices
- Know malicious software
- Malware reverse engineering and signature creation
- Identification of malware type, capability, target, and identification and remediation.
- Endpoint Management, Incident Response, eDiscovery, and Forensic capabilities
- Full Hard Drive and Memory Acquisition and Analysis
- Periodic Sweeps of Enterprise to baseline and identify new or changed entities, services,
- files and folders.

Penetration Testing

Yearly penetration testing of internet facing systems is occurring.

Security Health Checks

The Device Health Check is a professional review and thorough inspection of the device health and is based on ISO 27000 Security Standards and applicable CIS benchmarks, in combination with DJPaA’s extensive knowledge of security industry technologies & best practices for information security.

Web Application

Web Application Assessments are conducted several times during the software development lifecycle (SDLC) and at least quarterly for production systems or sooner if changes are made to the production software.

For more information contact payroll support at payroll@hrpro.com

1025 N. Campbell Road, Royal Oak, MI 48067 | hrpro.com | 248-543-2644 | Fax 248-543-2296 | newbiz@hrpro.com