Croner

HR • Tax • H&S • Reward

Croner Hosting Services

The Hosting Options, Process Controls and Security models used in Croner's web based software platforms*

croner.co.uk

*Excluding Simply Personnel

Hosting Options

Croner provides a data centre to provide an application platform that utilises the best of breed technologies in virtualization, data replication and security practices to provide a redundant primary data centre, with full site disaster recovery capabilities to a warm secondary site. This document will go into further detail around these hosting architectures, process and security controls in place.

Data Centre & Physical Security

Croner provides a robust, support and available IT platform, through a best of breed data centre.

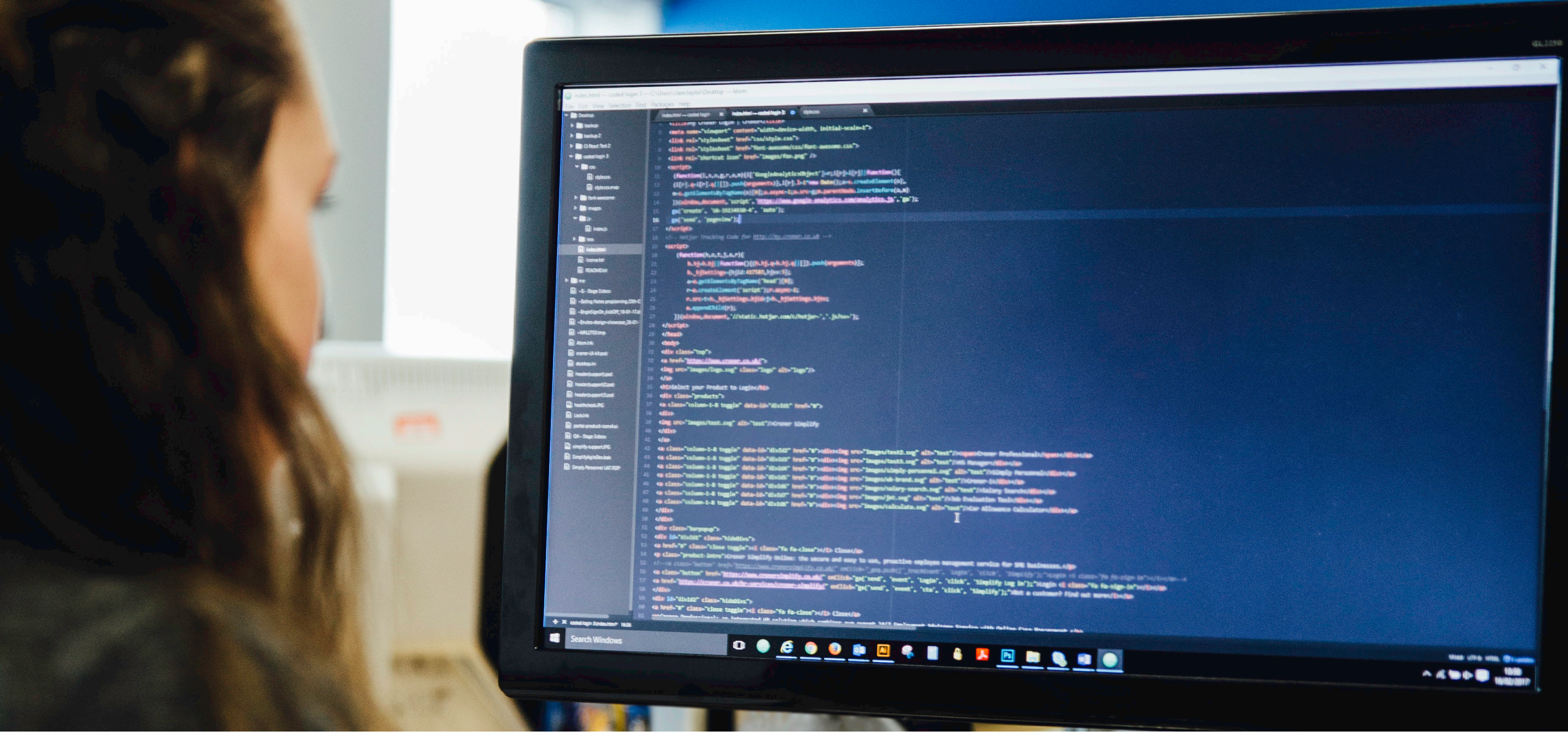
Key deliverables of this Data Centre provisioning include:

- Secondary, warm DR site at remote UK location
- Diverse fibre routing via multiple carriers
- Cross connection to a number of Tier 1 carriers
- Dual Power supply, UPS & onsite generator backup
- Fire, power, weather, temperature, and humidity monitoring.
- In the event of any problem, data centre NOC teams are on site 24 hours a day.
- ISO 9001:2008 & ISO 27001:2013 compliant.

All Croner hosted equipment sits on physical hardware that is completely dedicated to only running Croner services and the hosted solution is designed for full high availability – no single point of failure – providing truly enterprise class resilience.

The equipment is isolated directory services, ensuring that only allowed management servers or approved internal staff can access the servers. External access is limited to servers in a DMZ zone, with database servers being further segmented into a restricted security zone, using our full redundant firewall solution, which is only accessible by documented web servers on restricted TCP ports.

Data Centre access is restricted to the minimum number of staff who need access for operational purposes. Access logs are kept and audited monthly. Physical access is limited to remote hands staff and Systems Engineers, the list is limited to only those who require physical access to replace hardware. There are no console screens in the Data Centre permanently attached to any equipment.



Primary Site Disaster Recovery

Site disaster recovery is achieved by Croner maintaining a second UK based data centre.

Croner has designed a solution that utilises the latest technologies in virtualisation, SAN and database snapshot and replication.

The disaster recovery failover plan is tested annually.

Data Security & Access Control

Croner takes the security of our customer data extremely seriously, and all practical measures are made to ensure protection and appropriate access to your data at all times.

Server Access

Server access is limited to only Systems Engineers; this is handled remotely through Remote Desktop Connections or Virtualisation Administration Applications, which can only be initiated through a secure IPsec VPN tunnel from Croner sites. All access is on a named user basis and no generic accounts are used.

Database access is limited to Systems Engineers and Database Administrators, access is on a named user basis and no generic accounts are used. All named access is controlled by use of a dedicated Active Directory.

Server access passwords are changed every 42 days (6 weeks) with standard Microsoft Complexity requirements in place. Password minimum length is 8 characters. Croner Operational Management Review lists of staff that has access to sensitive customer information quarterly, to check for completeness and suitability for each member of staff current job role.

Application Access

Where passwords are sent to a user, they are set to expire and require change on first login.

Application and infrastructure penetration testing is performed at regular intervals by a third party, and Croner software development teams will respond to any highlighted security concern with planned work to eliminate or mitigate any exposed security vulnerabilities.

Data Encryption

In Transit

All data in transit from client browser to the Croner web application has forced encryption with only strong cipher suites enabled on the web server.

We use 2048-bit private keys on our certificates for optimum security.

At Rest

With the exception of passwords and specific sensitive personal details, data stored within SQL server is not encrypted due to performance degradation within the application. Croner rely on the security controls built into the application layer, coupled with tight control on who and how access is granted to the database layer to ensure your data is safe.

Data Backup Process

All production servers and data are backed up daily on an incremental basis and weekly on a full basis. These backups are retained for 2 months on a rolling cycle. Using the state of the art snapshot and replication technology deployed on the platform, these backups are replicated to our DR site, so there is redundancy on point in time backups as well as the Croner application across both sites. There are further monthly full backups to tapes which are retained on a 12 month rolling cycle.

Application Support

Our hosting service operate a 24/7 network operations centre, which will respond to any incidents that affect the performance application operating base line at the data centre.

Croner has a dedicated in-house technical application support team which will answer all initial customers' queries and resolve or escalate as required to other Croner technical teams.

Application Monitoring

Croner have engaged with a leading cloud application monitoring program so that at an application level, Croner's support and development teams have the deepest insight into the workings of the software's production platform.

This allows for faster end-to-end transaction tracing, exception reporting on key transactions and allows our support teams to easily establish acceptable application performance baselines and to know if the application performance falls below it.

Server Management

Vulnerability management and patching

Patch management is handled via Internal WSUS servers. All patches are tested on development and test servers before being promoted onto production.

Exceptions can be made for critical patching where the risk is deemed too great not to apply it immediately. In the packages are still tested on development and test servers, however the testing period is shortened to 24 hours.

Changes to the System

In a dedicated system instance, all system updates/upgrades run through an approval and communications process which involves notification of designated client contacts of planned system downtime. Downtime is negotiated with the customer with the exception of critical issues.

Logging and monitoring

All Production servers are monitored on a 24/7 basis using industry standard applications. In the event of an incident, on call staff are notified by emails and support tickets are automatically raised.

Release Management

Application Enhancement and Review

System enhancements are built into Croner Products using a standard Agile software development methodology. We use a consultative approach of involving clients heavily in determining system requirements which are then turned into specifications which are then in turn prioritized for release and included into the product roadmap. Once a software release commences, agreed scope items are worked through using an Agile approach to develop and test in 3 week sprints. At the completion of the development sprints, end to end testing is performed to ensure the accuracy of both new enhancements and the existing system functionality. Software is then packaged and released and often beta tested by designated clients.

Security is ensured via code reviews, standards reviews and thorough testing of all new and revised components that link into the security model of the application.

Infrastructure Patch Review

All Operating System, DBMS and Virus software updates are reviewed and applied according the evaluated need and associated risk of non-application. Servers that are used for load balancing or as test or staging sites are synchronised in terms of patched version of OS and underlying software.

Simply Personnel GDPR and Data Protection Q&A

Data Protection Compliance

Will you be in a position to meet your obligations as a data controller or processor (as applicable) under the GDPR by 25 May 2018?

Yes. Croner currently processes all personal data in accordance with the Principles of the Data Protection Act 1998. Croner is aware of GDPR and its obligations and are currently considering our position in relation to it and the compliance manager is driving the project forward. Any required changes will be implemented before May 2018 to ensure we are as compliant by 25th May 2018.

Do you have a DPO? Please provide details. If you do not have a DPO who is responsible?

Yes. Gail Tuck: Group Compliance Manager.

Do you have GDPR-compliant data protection and information security policies?

No. All policies and procedures are compliant with ISO27001. We are in the process of reviewing and finalising our policies and procedures to ensure that they will be GDPR compliant by 25th May.

Will you be providing training to your staff on compliance with the GDPR? If so, please provide details.

Yes. Training is already in progress. The whole business will receive GDPR training and more in-depth training will be provided for managers as required.

IT Security Policy

Who is responsible for IT Security in the organisation? Please provide details.

Mark Winstanley. Information Security Manager mark.winstanley@peninsula-uk.com
Rob Smith. Head of IT rob.smith@croner.co.uk
Gail Tuck. Group Compliance Manager gail.tuck@peninsula-uk.com

Does an IT security policy exist and, if so, how is it communicated to employees?

Yes. During induction training and reinforced periodically during training sessions throughout the year.

What policies and procedures do you have in place for immediate reporting and investigation of suspected data security breaches, and remedial action in respect of actual breaches? Do you have a data security breach policy?

Yes. Data Protection Policy and a Data Breach policy.

Is your organisation compliant and certified for any recognised IT Security and Data Protection standards.

Yes. Croner is ISO27001 certified and holds Government accredited Cyber Essentials certification (Certificate Number: 1089522795658013).

Physical Security

How is the physical security of buildings providing Information Services to the company ensured.

Yes. The reception is staffed 24/7. A door access control system is in place throughout the building and all entrances are monitored by CCTV including the Data Centre.

What specific precautions are used to ensure only authorsed access to areas containing data processing, communications and storage equipment used for company data.

Yes. Secure areas are protected by appropriate entry controls to ensure that only authorised staff are allowed access. Staff requiring access to secure areas are to limited to the minimum required and their access removed when their employment ends or move roles. They are issued with an access control card that allows them entry. CCTV monitoring is deployed at all access points.

Do you have a Disaster Recovery/Business Continuity plan? If so, When was the last test and what were the results? Has all necessary remediation been carried out and retested?

Yes. A BCP/DR policy has been implemented. While a full annual DR test is not possible individual components are tested on a regular basis. All necessary remediation has been carried out.

Staff Security

Do you have a dedicated team to support Information and Cyber Security?

Yes. As part of the Peninsula Group, Croner has a dedicated InfoSec team with network security SIEM platform and incident monitoring.

How are Croner staff screened prior to employment?

Yes. CV and phone screening. Face to face interview. Induction in data protection. Staff qualifications checked for validity and membership to professional bodies.

Do Employment Terms & Conditions cover information security responsibilities including data protection?

Yes. These are included in the Employee handbook which is issued to all new employees.

Do these contain confidentiality clauses?

No. However, a Restrictive Covenant is signed prior to employment. All staff are then required to sign a confidentiality agreement on the first day of their employment. Also contained within the employee handbook.

Please explain the approach to ensuring that staff are adequately trained in IT Security and Data Protection principles.

Yes. All staff receive security training as part of induction. This is reinforced periodically during training sessions and presentations.

What is the internal process for reporting and managing security incidents?

Yes. All security incidents are managed by the InfoSec team and logged and investigated accordingly.

How quickly is Croner staff access revoked on them leaving employment?

Yes. Immediately. Croner have a leavers policy in place, in which a leaver form is circulated to a group of system administrators with a termination date. The system administrators disable the accounts, blocking all access on the date specified.

What protection is in place to ensure that staff credentials are not compromised by malware, remote access tools, keyboard loggers etc.?

Yes. On Croner networks, antivirus and malware protection is deployed on all endpoints to detect, alert and neutralise these threats.

Data Security

What Operating Systems are in use and what steps are taken to ensure they are protected?

Yes. Croner desktops and laptops use Windows 10 or Windows 7. A rollout is in progress to move all endpoints to Win10. Windows updates are pushed out and installed automatically.

How is it ensured that software used to process company data is kept up to date.

Yes. On Croner equipment, all software is managed and patched centrally. Only approved software is permitted on user machines and updates are managed through Software Centre.

Will vendor staff ever carry company data on portable devices (inc storage media)? If so how will the data be protected from loss/theft?

No. This is prohibited. However, all laptops are encrypted for added protection.

What measures are in place to prevent unauthorised access to Data from outside “hackers” (eg firewalls and other security measures) and to what extent is the adequacy of current precautions monitored?

Yes. External connections are protected with enterprise, resilient firewalls and dedicated security monitoring ex. SIEM, IDS, IDP

What restrictions are in place to ensure control of data entering or leaving via internet access (via web browser, email, ftp, online storage etc)?

Yes. Internet access is controlled by a dedicated Web filtering appliance which restricts the types of traffic and URLS. Firewalls and monitoring control and monitor traffic entering and leaving the organisation.

Which Applications will host company Information? Please identify any in use which are not fully supported by the software provider.

Yes. Salesforce is the primary platform for Croner controlled data. No sensitive information would be stored on unsupported systems.

How are application patches evaluated, tested and deployed?

Yes. On Croner equipment, all patches are governed by the Change control process which includes evaluation, testing and deployment.

Software application changes are managed through a standard Agile software development methodology. Once a change is completed, end to end testing is performed to ensure the accuracy of the change and the existing system functionality. Software is then packaged and released, and often beta tested by designated clients.

What security mechanisms are in place to protect access to the company's data?

Yes. On Croner equipment, all access is controlled through ADS permissions and access is granted on the principle of least access. Security monitoring has been deployed including a dedicated SIEM platform. On third party hosting platforms, penetration testing is carried out at network level on a regular basis.

What are the password complexity requirements?

Yes. All passwords must be unique and complex: eight characters minimum with one small case, capital letter, symbol and number.

How often are passwords forced to change?

Yes. On Croner systems, password changes are enforced every 30 days.

Are idle time screensaver locks enforced for all Croner staff? If so what is the timeout?

Yes. Idle time screensaver apply after 2 minutes.

Can you confirm that all default admin and application backdoor accounts have been removed?

Yes. A standard build procedure ensures that all default admin and backdoor accounts are removed. Network monitoring identifies any non-compliance.

For systems, which are accessible to users from the Internet, what precautions are taken to prevent the existence and exploitation of web application vulnerabilities such as cross-scripting or SQL Injection.

Yes. A dedicated web application firewall protects the application from malicious actors and vulnerabilities such as cross-site scripting and SQL injection. External facing websites are scanned regularly to identify any vulnerabilities, which are addressed immediately.

Where is information stored?

Yes. For Croner controlled data, it is held within the secure CRM platform (Salesforce).
For Client controlled data, it is held within a client specific database.

How is access secured?

Yes. Croner internal network access is controlled through internal Active Directory security. Croner access to Salesforce is accessed via https secure internet browser.

Client access to the web application is controlled by user credentials defined by the client administrator within the software application.

Is the data encrypted?

Yes. Full database encryption is in place and secure SSL web access for client portal access

If so how is the encryption key managed

Yes. Encryption keys are managed in accordance with strict policies and procedures. The key is stored in a secure location which is accessible only to database admins.

Is a Data Loss Prevention in place.

No. Data Loss Prevention is currently managed by policies, procedures and controls. However, a dedicated DLP appliance will be deployed in the near future to Croner networks (excluding third party platforms).

Backup System

How is data backed up?

Yes. Croner controlled data is backed up continuously through the high availability platform. In addition, all data is backed up to physical media daily. Client controlled data is backed up continuously through the high availability platform with additional hourly snapshots. Backups are retained on a rolling two week basis.

How is access to backup data secured?

Yes. Physical backup media is encrypted using AES256 bit encryption

How often will data be backed up?

Yes. Croner controlled data is backup to physical media on a daily basis.

How often is the data restore process tested?

Yes. The restore process for Croner controlled data is tested monthly or as required.

What other measures are in place to ensure data integrity and continuity?

Yes. File integrity monitoring is in place for Croner controlled data.

Backup System

What controls are in place for making local copies of data on PC Hard Drives/USBs/DVD-RW etc.?

Yes. On Croner equipment local copies are not allowed. This policy is enforced through Microsoft Group Policy and Kaspersky device control.

Please explain any policies or circumstances that could lead to company data being held on employees personally owned devices and controls over this.

Yes. The written policy states clearly that this is forbidden and this policy is enforced through technological controls. InfoSec and Director approval is required for any policies exceptions

Will personal data be stored and/or processed on equipment outside of vendor premises? If so please give details of how and where together with associated security controls?

Yes. Some employees work from home and use corporate laptops, which are locked down and protected by antivirus and all corporate security policies.

What is your retention/deletion policy that applies to personal data?

Yes. Croner controlled data is retained in line with Croner's Retention Policy. Therefore we are committed to taking a practical approach in line with legal, contractual and commercial requirements when dealing with the ownership, retention and disposal of information relating to our business activities within the UK and Ireland. Data is destroyed/deleted when we no longer have legal, contractual or commercial requirements to hold the data.
Client controlled data should be retained in line with the client's data retention policy.

Are there any circumstances in which a copy of any personal data is stored after the end of the services?

Yes. Only as per the data retention policy

How is paper information containing company data destroyed?

Yes. Confidential waste bins are located on each floor and this is securely shredded by a vetted third party.

Cloud Services & 3rd Party Access

Does your organisation use Cloud Storage facilities for processing data?

Yes. Croner's web applications are built on secure cloud infrastructure hosted by Croner.

How is security maintained and tested?

Yes. Security is managed by a dedicated security team which regularly tests and verifies that all controls are operational.

Does all data reside in the EU?

Yes. All data resides in a Primary and secondary Data centre which are both based in the UK.

Has any Penetration testing been performed in the past 12 months?

Yes. Penetration testing is carried out at network level on a regular basis. Testing at client virtual machine level can be organised by the client in conjunction with our infrastructure team.