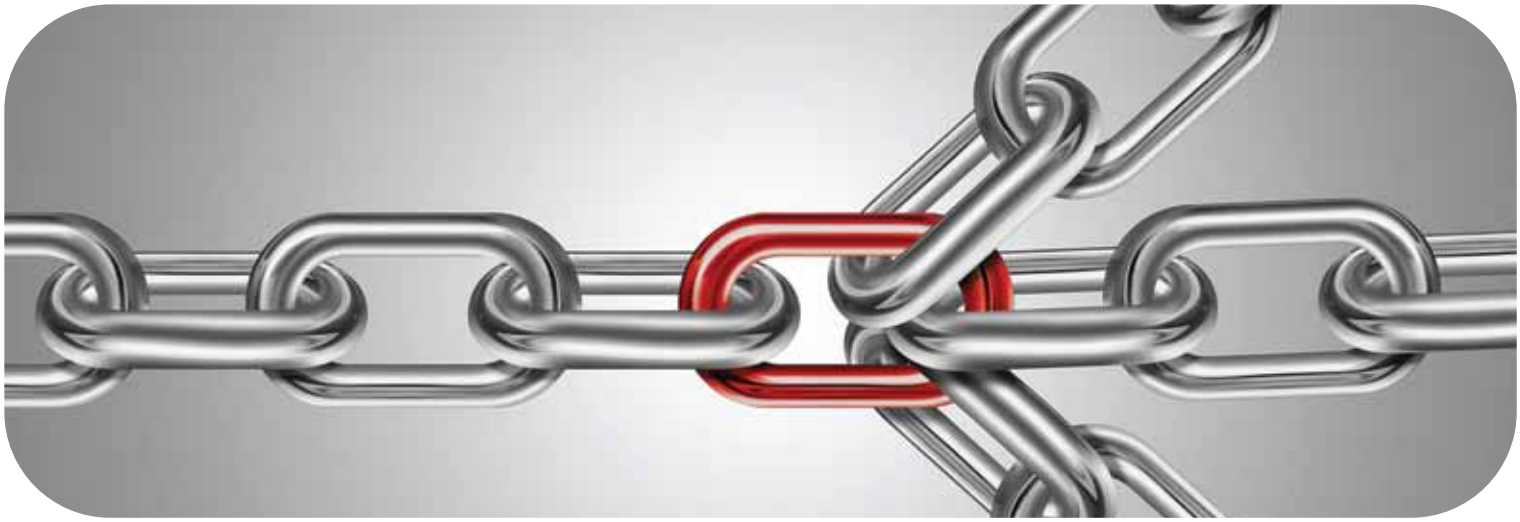


Chronologic data protection statement

System: Citadel cloud-based time and attendance system

Our commitment to data protection

In common with all UK businesses, we aim to comply with current data protection legislation and any changes to that legislation. The protection of data provided by our customers for their own use on a Citadel system is considered to be as important as protection of Chronologic's own customer data. Both are critical to the operation of our business. We take our common responsibility to protect shared data very seriously and regularly review what we can do to mitigate the risk of data loss.

Data protection is a common responsibility

Time and attendance systems are designed to contain personal data obtained by an employer as part of the employer / employee relationship. Access to that data must be restricted and all parties with access to it must comply with data protection legislation, which includes the **UK Data Protection Act 1998 and the EU General Data Protection Regulations** (GDPR) effective from 25 May 2018.

All parties that have access to a Citadel account share a common responsibility for security and compliance with data protection legislation. This includes the input of data into the system, processing and storage of data and outputs such as reports.

This Data Protection Statement sets out our understanding of the data flows and access between our organisation and a customer's, and the responsibilities for the protection of that data that are put in place.

The Citadel system

The Citadel system is owned and developed by Workwell™ Technologies, a US company. Chronologic is a business partner of Workwell™ Technologies Inc. and is responsible for sales, marketing, system configuration, training and support for our customers in the UK and Europe.

The Citadel time and attendance system software is installed on servers in the Amazon Web Services (AWS) data centre. Each customer sets up and controls access to their Citadel online account, populates it with employee information and manages that information.

It is the responsibility of Chronologic's customers to maintain the security of access to their Citadel account system. Password protection is built into the system. System administrators need to observe password security disciplines. Customers need to apply the data protection measures they already have in place for their own IT systems to the Citadel account system.

Personal data held on a Citadel account system

Data input

The range of personal employee data held is determined by our customers. Standard information includes first and last names, email address, phone number, payroll number and base pay hourly rate.

Clocking in data can be input into the system using a wide range of options including:

- Fingerprint and facial recognition terminals; RFID proximity fob terminals. Terminal connections can be wired i.e. plugged into your network or WiFi.
- Self-service web clocking for PC, Mac, tablet or smartphone. Using a PIN (personal identification number) and geolocation.
- Smartphone clocking using an Android or IOS app.

Clocking terminals located on customer or third-party premises collect clocking data. The terminals synchronise with the server every time there is a clocking event. This clocking data is associated with a personal identifier corresponding to an individual employee and is transmitted in an encrypted format. No clocking data is stored in the clocking terminals.

The smartphone clocking apps comply with the relevant Google security standards. The risk of interception of data packets and data loss for individual clocking instances is considered to be negligible.

Data output

The output of personal data from the Citadel online account is controlled and managed by the customer. Access to the system is managed by the customer's administrator/s and is password protected.

Customers are able to export data and reports from the system either as CSV or PDF files or in emails.

Chronologic access to customer data

Chronologic is a business partner of Workwell Technologies Inc. and is responsible for sales, marketing, system configuration, training and support for our customers in the UK and Europe. As the development partner for the system, Workwell may need to access employee data to ensure functionality is working correctly and that reports access and manipulate the data accurately. Workwell will be EU-US Privacy Shield certified when GDPR becomes effective on 25 May 2018.

Chronologic has access to:

- Citadel online accounts via an administration portal.
- A monitored desktop sharing program called ISL.

Trained employees in Chronologic's Customer Support team have access to customer's employee data for support purposes only (Chronologic do not use outside contractors). Chronologic do not allow system access to customers' sub-contractors when they are employed to provide installation services; all system configuration is carried out remotely by Chronologic staff.

Chronologic maintain strict IT procedures and security methods to protect its own IT infrastructure.

AWS access to customer data

AWS could in theory access Citadel accounts, although they have no reason to do so. AWS will be GDPR compliant when it becomes effective on 25 May 2018.

Risk of data loss

Risk of data loss can be divided into two main areas:

1. **Human error resulting in unauthorised access to system credentials or unauthorised disclosure of data or reports containing data.**

    - Unauthorised access to or use of the system by personnel due to lack of password control/security.
    - Lack of data security for reports and data exports distributed within the customer environment.

Customers

Access to a Citadel account is locked with a Username and Password. The self-management of the system enables customer administrators to create and manage their own access levels within the system. This process needs to be managed through the customer's own IT policies and procedures.

Reports can be generated by the system detailing a range of information from an employees' hours, to their email address and phone numbers. Reports that are generated and / or printed by customers are subject to their own IT, security and data protection policies and procedures.

Chronologic

Chronologic relies on its operating procedures, and the experience and training of its staff to ensure that account credentials and other information are not inadvertently released to unauthorised parties.

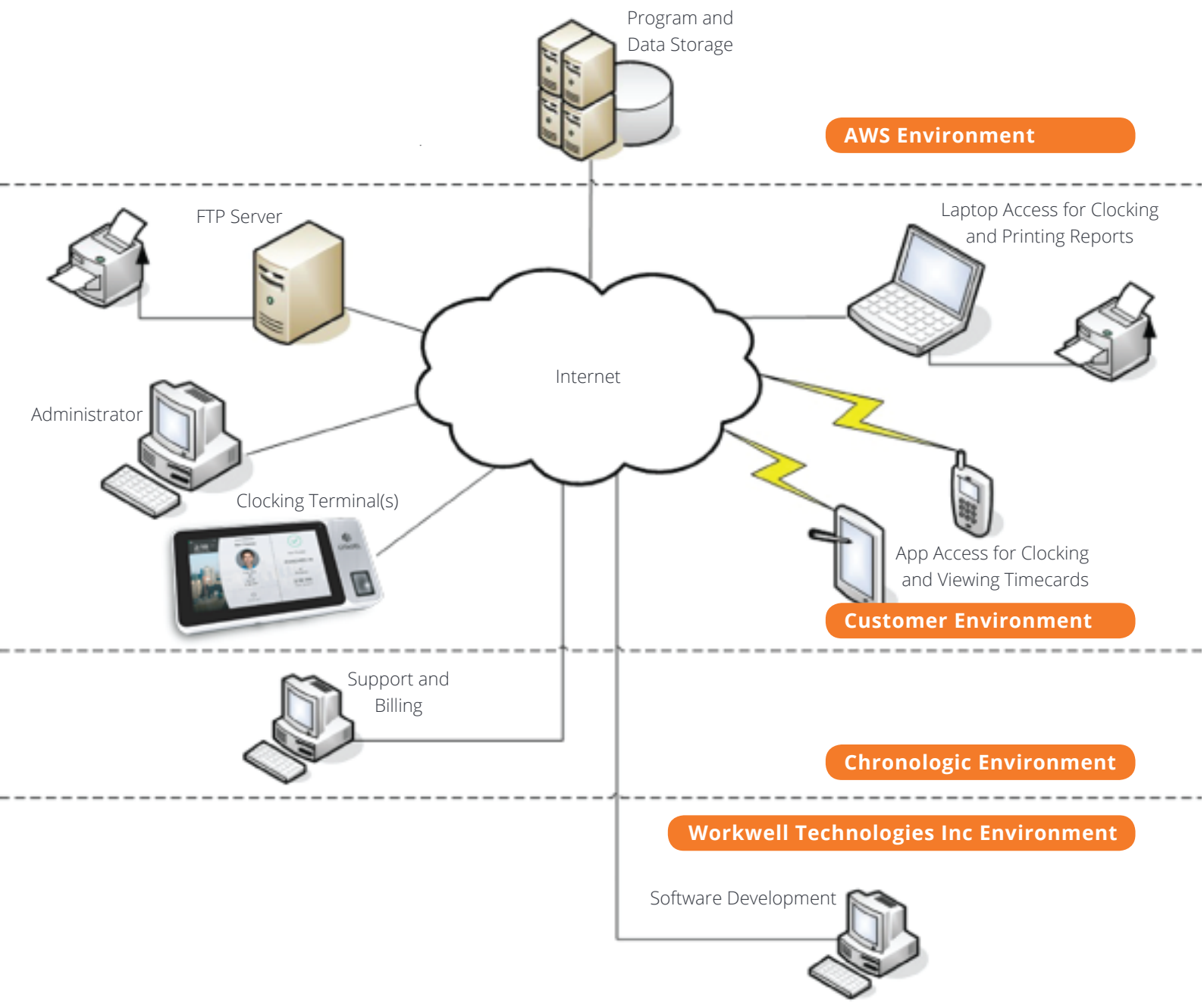
Chronologic system development and support staff have access to a customer's system and access it when required to provide support to customers.

Chronologic may on occasion run a report as part of support activity. If these reports need to be retained, storage is strictly controlled and subject to Chronologic's IT, security and data protection policies and procedures. If these reports need to be destroyed, they are shredded on-site using a heavy duty cross-cut shredder.

2. **Any vulnerability of the system to incursions by third parties to capture data.**

The risk of loss of personal data by incursions into the Citadel account resulting in a data breach are considered to be extremely low because of the way in which the system is implemented and operated.

The standard employee information held on the system is likely to be of limited commercial value.



More information

If you would like further information about security aspects of your Citadel account or need help setting up access levels please get in touch.

For general information about Data protection and GDPR visit the Information Commissioner's Office (ICO) website.