Data Security Policy

April 2018 Version 8.3

Table of Contents

Summary & Overview

Information management is an essential part of good IT governance, which in turn is a cornerstone in corporate governance. An integral part of the IT governance is information security, in particular pertaining to personal information.

This document combines legal requirements and current best practice for an information security management policy. It provides information on security objectives and strategy and defines roles and responsibilities.

Core principles for information security management, as defined in ISO/IEC 27002, are for the following areas:

- Risk Assessment
- Access Control
- Organising Information Security
- System Development and Maintenance
- Asset Management
- Information Security Incident
- Human Resources Security Management
- Physical Security
- Business Continuity Management
- Communications and Operations
- Compliance Management

Introduction

This document contains Cloud9 Software information security policy. It is based on ISO/IEC 27001 and ISO/IEC 27002, the Director of Cloud9 Software has signed the security policy.

In addition to the information security policy Cloud9 Software have developed several underlying documents detailing how the various aspects of the policy is implemented. These are referenced within in the present document.

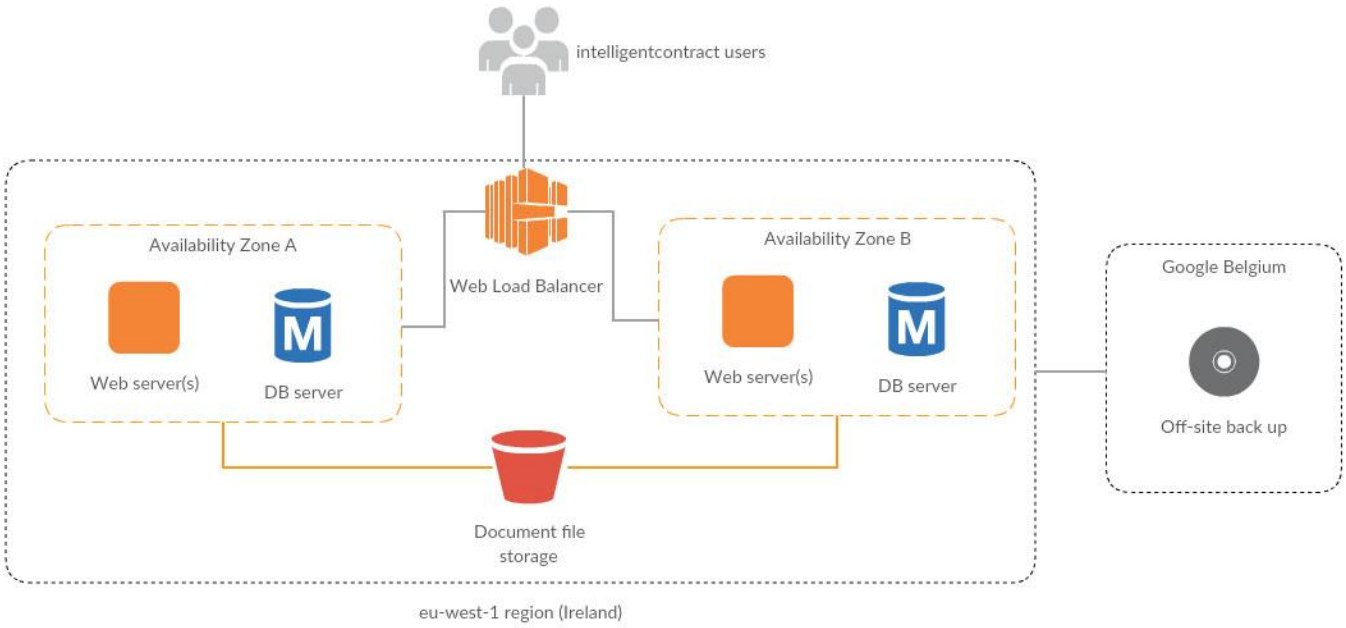
Cloud9 Software Data Security Overview

The use of Cloud-based solutions is becoming more prevalent, predominantly due to the substantially lower cost of ownership and flexibility offered when compared with traditional “installed” software. However, there is a key concern for customers surrounding the security of their data: both the unauthorised access to data and the loss of any data.

At Cloud9 Software (C9S) we realise the importance of data security to our customers, so we have taken measures so that we and our partners have policies, procedures and systems in place to reduce the security risks relating to your data. We are committed to ensuring that your information is secure and prevent unauthorised access, disclosure or loss of your data. In this product data sheet, we describe the application level security, hosting partner policies and procedures and backup and recovery procedures we have put in place to safeguard and secure the information we hold on your behalf.

Overview of our Platform Architecture

Intelligentschedule.com is hosted by Amazon Web Services (AWS). AWS is a tier 1 web hosting service. Intelligentschedule.com is hosted out of AWS’ Dublin facility in Ireland. There are two physical locations (availability zones) which provide a level of redundancy within our architecture. The diagram below provides an overview of the intelligentschedule.com technical platform.



Application Security

We take the security of our application very seriously. We employ an external party on an annual basis to review our application security arrangements. The annual penetration test is completed in the first quarter of each year and the annual results can be provided upon request.

The intelligentschedule.com application has built-in security measures that provide peace of mind to our customers. The table below provides information on the key measures that have been implemented.

Measure	Purpose
Application is only available over HTTPS (additionally HSTS is enabled and cookies are flagged as HTTPS only)	Prevents attackers from accessing sensitive data by sniffing network traffic
Application is hardened against XSS, clickjacking, CSRF and SQL injection attacks (verified by penetration testing)	Prevents attackers from executing harmful code on the server or tricking legitimate users' browsers into giving away login credentials or data
Customer-configurable login session timeout	Customers can optionally specify a time after which inactivelogin sessions should time out
Customer-configurable password strength	Customers can switch on a "strong passwords" setting which forces users to use complex passwords
5 failed login attempts allowed in 5 minutes before Captcha image is presented. The account is locked if there have been 10 failures in the last 5 minutes	Prevents non-authorised people (maybe who are using brute force attacks) from attempting to guess passwords.

Customer - configurable password options to expire users' password after specified length	If a customer doesn't restrict access to an ex-employee's login,after the specified period access will automatically be revoked
Forgotten password functionality requires users to confirm password reset via a link sent to their email account	Prevents attackers from resetting users' passwords without their consent
IP address and time/date of most recent login displayed to user on login	Alerts users if their account has been logged in to from an IP ata time and date they don't recognise
Read/write access to entities within the system (Contracts, documents etc.) can be locked down to specific users and groups of users	Allows Customer to control who within their organisation can access which data
User file uploads are restricted to specific file types	Prevents users from uploading harmful files including as viruses

Hosted Environment Security

Our hosting partner has security measures in place that adhere to the data security standard ISO270001. A detailed copy of AWS' security white paper can be obtained on request. In addition to AWS hosted environment security measures, we have implemented further security measures designed to prevent.

Measure	Purpose
2-factor authentication required to access back-end C9S administration portal	Prevents attacker who's acquired a password to the system from gaining access
Access to live servers and database administration interface restricted to C9S office IP address	Prevents anyone outside the C9S network from accessing the hosting infrastructure
Firewall and load balancer in place	Clients cannot connect directly to the live servers or database but must come through a load balancer. Only the ports that strictly need to be opened (HTTP/HTTPS) are accessible.
Staff with access to the C9S administration portal have signed Non-disclosure agreements, are back ground checked annually (Disclosure Scotland) and are made aware annually of the consequences of breaking the terms of the Non-disclosure agreement.	Because employees have access to data it is important that those staff are able to demonstrate they are trustworthy and also for them to be aware of the consequences of unauthorised disclosure. The NDA agreements apply after an employee has left the business
It is our policy that customer data should not be downloaded to local computers or any type of portable media	By having a policy that customer data only ever resides in the data centre we are able to minimise the risk of unauthorised access of customer data
The C9S office is physically secured with a combination lock. No one is allowed into the office unless a background checked member of staff is present.	Removes the risk of opportunistic individuals accessing machines which may have access to the data centre
We are able to demonstrate that we comply the UK data protection (acting as a processor).	To give our clients piece of mind that personal data is treated in line with the stipulations of the UK data protection act.

Backup and Recovery Strategy

Customer Meta data

SQL databases in AWS are backed up on an on-going basis with backups retained for 30 days. Point in-time recovery is available with these backups so we can restore to any point in time within the previous 30 days. Additionally, the databases are converted to text files once a day and these are backed up to a file storage area within our AWS account.

Customer Uploaded files

Files uploaded by Customers (for example, contract documents) are incrementally backed up on an hourly and daily basis to the file storage area within our AWS account. These incremental backups cover a period of 2 weeks so in the event of data being lost from our primary file storage, we can restore to the nearest hour at any point within that period.

On a weekly basis, the database dumps and file backups are archived to a weekly backup directory within the AWS file storage area, and these weekly backups are retained for two years. Finally, all data stored within the AWS file storage area (including historical backups) is incrementally backed up on a daily basis to a secure storage area within a separate storage (Google Cloud Storage) account. This is also retained for 2 years

Note that the AWS file storage is located in Dublin, Ireland and the Google cloud storage is located in Belgium.

Disaster Recovery

Customer data is primarily located our AWS facility in Dublin Ireland. We have reserved space in two physically separate locations – should there be an issue in one location, service will automatically switch over to the other.

We have a documented disaster recovery procedure which covers both the C9S office location and the AWS data centre. The plan is rehearsed on an Annual basis and alterations made if required.

Policy Amendments

Any changes, edits and updates made to the data Security Policy will be recorded in here. Whenever there is an update, Cloud9 Software requires that the version number be updated and the key reasons for change be recorded.

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
Judy Weeks	Contributor	2-Apr-2016	1.0	Initial version of DSR
Paul Darlow	Data Protection Officer / Director.	23-Apr-2018	2.0	Updated to take into account the new legislation around GDPR.

1 Information Security Policy

1.1 Security Goals

Cloud9 Software is committed to safeguard the confidentiality, integrity, and availability of all physical and electronic information assets of the institution to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security at Cloud9 Software are the following:

- Ensure compliance with current laws, regulations, and guidelines.
- Comply with requirements for confidentiality, integrity and availability for Cloud9 Software's employees, and Customers.
- Establish controls for protecting Cloud9 Software's information and information systems against theft, abuse and other forms of harm and loss.
- Motivate employees to maintain the responsibility for, ownership of and knowledge about information security, to minimise the risk of security incidents.
- Ensure that Cloud9 Software can continue their services even if major security incidents occur.
- Ensure the protection of personal data (privacy of data both as a "data processor" and spefic subjects).
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by Cloud9 Software.
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001.
- Ensure that external service providers (sub-processors) comply with Cloud9 Software's information security needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems from outside our data centre.

1.2 Security Strategy

Cloud9 Software's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating, and controlling information related risks through establishing and maintaining the information security policy (this document).

It has been decided that information security is to be ensured by the policy for information security and a set of underlying and supplemental documents. To secure operations at Cloud9 Software even after serious incidents, Cloud9 Software shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.

The term information security is related to the following basic concepts:

- ***Confidentiality:***

The property that information is not made available or disclosed to unAuthorised individuals, entities, or processes.

- ***Integrity:***
  The property of safeguarding the accuracy and completeness of assets.
- ***Availability:***
  The property of being accessible and usable upon demand by an Authorised entity.

Some of the most critical aspects supporting Cloud9 Software's activities are availability and reliability for network, infrastructure, and services. Cloud9 Software practices openness and principles of public disclosure but will in certain situations prioritise confidentiality over availability and integrity.

Every user of Cloud9 Software's information systems and employees shall comply with this information security policy. Violation of this policy and of relevant security requirements will therefore constitute a breach of contract between the user and Cloud9 Software and may have consequences for employment or customer contractual relationships.

2 Roles and Areas of Responsibility

The Managing Director of Cloud has the overall responsibility for managing Cloud9 Software's values in an effective and satisfactory manner according to current laws, requirements, and contracts.

The Director has the overall responsibility for information security at Cloud9 Software, including information security regarding personnel and IT security.

2.1 Owner of the Security Policy

The Managing Director is the owner of the security policy (this document). The Director delegates the responsibility for security-related documentation to the CSO (Chief Security Officer). All policy changes must be approved and signed by the CSO. Paul Darlow is the Managing Director.

2.2 Chief Security Officer (CSO)

The Chief Security Officer (CSO) holds the primary responsibility for ensuring the information security at Cloud9 Software. **Paul Darlow**, Managing Director, has this role.

2.3 System Owner

The system owner, in consultation with the IT department, is responsible for purchasing requirements, development and maintenance of information and related information systems. All systems and all types of information has a defined owner. The system owner defines which users or user groups are allowed access to the information and what authorised use of this information consists of.

Mike Edwards, Technical Director is owner of the Intelligentschedule.com system (This includes the front-end portal and the back end application)

2.4 System Administrator

System administrators are persons administrating Cloud9 Software's information systems and the information entrusted to Cloud9 Software by other parties. Each type of information and system may have one or more dedicated system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is not lost. They will further implement, run, and maintain the security systems in accordance with the security policy. Each system must have one or more system administrators.

Mike Edwards, Technical Director is the System Administrator for Intelligentschedule.com

2.5 Internal Technical Staff

Employees are responsible for getting acquainted and complying with Cloud9 Software's IT regulations. Questions regarding the administration of various types of information are posed to the system owner of the relevant information, or to the system administrator.

2.6 Consultants and Contractual Partners

Contractual partners and contracted consultants must sign a confidentiality agreement prior to accessing sensitive information. The System owner is responsible for ensuring that this is implemented.

3 Principles for Information Security at Cloud9 Software

3.1 Risk Management

3.1.1 Cloud9 Software's approach to security will be based on risk assessments.

3.1.2 Cloud9 Software will continuously assess the risk and evaluate the need for protective measures. Measures will be evaluated based on Cloud9 Software's role and with regards to efficiency, cost, and practical feasibility.

3.1.3 An overall risk assessment of the information systems will be performed annually.

3.1.4 Risk assessments will identify, quantify, and prioritise the risks according to relevant criteria for acceptable risks.

3.1.5 Risk assessments will be carried out when implementing changes impacting information security. Recognised methods of assessing risks will be employed, such as ISO/IEC 27005.

3.1.6 The CSO is responsible for ensuring that the risk management processes at Cloud9 Software are coordinated in accordance with the policy.

3.1.7 The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.

3.1.8 Risk management is to be carried out according to criteria approved by the management at Cloud9 Software.

3.1.9 Risk assessments will be approved by the management at Cloud9 Software and/or the system owners.

3.1.10 If a risk assessment reveals unacceptable risks, measures will be implemented to reduce the risk to an acceptable level.

3.2 Information Security Policy

3.2.1 The CSO will ensure that the information security policy, as well as guidelines and standards, are utilised and acted upon.

3.2.2 The CSO will ensure the availability of sufficient training and information material for all users, to enable the users to protect Cloud9 Software's data and information systems.

3.2.3 The security policy shall be reviewed and updated annually or when necessary, in accordance with principles described in ISO/IEC 27001.

3.2.4 All important changes to Cloud9 Software's activities, and other external changes related to the threat level, will result in a revision of the policy and the guidelines relevant to the information security.

3.3 Security Organisation

Security responsibility is distributed as follows:

- The CSO is primarily responsible for the security and is the controller according to the 95/46/EC, Article 2 (d).
- The security authority at Cloud9 Software, including information security and IT security, has been delegated to Paul Darlow is hereby appointed CSO (Chief Security Officer) at Cloud9 Software.
- Each System Owner is responsible for implementing the unit's information security. The managers of each unit must appoint separate security administrators.
- The CSO has the primary responsibility for the information security in connection with Customer related information.
- The System administrator has executive responsibility for information security in connection with IT systems and infrastructure.
- The System Administrator has executive responsibility for information security in connection with structural infrastructure.
- The Human Resources Manager has executive responsibility for information security according to the Personal Data Act and is the controller daily of the personal information of the employees. This is Vicky Basnett.
- The Human Resources Manager has executive responsibility for information security related to HSE systems.
- The CSO has executive responsibility for research related personal information.
- The System Owner manager has overall responsibility for quality work, while the operational responsibility is delegated according to the management structure.
- Projects is Organised according to Cloud9 Software's project process.
- Cloud9 Software's information security will be revised on a regular basis, through internal control and at need, with potentially assistance from an external IT auditor.

Cloud9 Software has established a forum for information security consisting of the system owner, the Human Resource manager and others if required. The security forum will advise the CSO about measures furthering the information security of the Organisation. The security forum has the following responsibilities, among others:

- Review and recommend information security policy and accompanying documentation and general distribution of responsibility.
- Monitor substantial changes of threats against the information assets of the Organisation.
- Review and monitor reported security incidents.
- Authorise initiatives to strengthen information security.

3.4 Classification and Control of Assets

3.4.1 "Assets" include both information assets and physical assets.

3.4.2 Information and infrastructure will be classified according to security level and access control.

3.4.3 Information as mentioned in item 3.4.1 will be classified as one of three categories for confidentiality:

Sensitive
Information of a sensitive variety where unauthorised access (including internally) may lead to considerable damage for individuals, Customers or their interests. This type of information must be secured in "red" zones, see chapter 3.6.

Internal
Information which may harm Cloud9 Software or be inappropriate for a third party to gain knowledge of. The System owner decides who may access and how to implement that access.

Open
Other information is open.

3.4.4 Cloud9 Software shall carry out risk analyses to classify information based on how critical it is for operations (criticality).

3.4.5 Routines for classification of information and risk analysis have been developed.

3.4.6 Employees administrating information on behalf of Cloud9 Software will treat said information according to classification.

3.4.7 Sensitive documents are all clearly marked.

3.4.8 Classification of equipment according to criticality will be discussed in chapter <chapter>.

3.4.9 A plan for electronic storage of essential documentation should be developed.

3.4.10 Information that is vital for operations should be accessible independent of which systems the information was created or processed in.

3.5 Information security in connection with Employees of Cloud9 Software's services

3.5.1 Prior to employment

3.5.1.1 A background check (Disclouse Scotland, Basic) is carried out of all appointees to positions at Cloud9 Software according to relevant laws and regulations.

3.5.1.2 A confidentiality agreement is signed by employees, contractors or others who may gain access to sensitive and/or internal information.

3.5.1.3 IT regulations should be accepted for all employment contracts and for system access for third parties.

3.5.2 During employment

3.5.2.1 The IT regulations refer to Cloud9 Software's information security requirements and the employees' responsibility for complying with these regulations.

3.5.2.2 The IT regulations should be reviewed regularly with all employees and with all new hires.

3.5.2.3 All employees and third-party employees receive adequate training and updating regarding the Information security policy and procedures. The training requirements may vary.

3.5.2.4 Breaches of the Information security policy and accompanying guidelines will normally result in sanctions.

3.5.2.5 Cloud9 Software's information, information systems and other assets will only be utilised for their intended purpose. Necessary private usage is permitted.

3.5.2.6 Private IT equipment in Cloud9 Software's infrastructure may only be connected where explicitly permitted. All other use must be approved in advance by the IT department.

3.5.2.7 Use of Cloud9 Software's IT infrastructure for personal commercial activities is under no circumstances permitted.

3.5.2.8 Employee background checks are completed annually (January of each year)

3.5.3 Termination or change of employment

3.5.3.1 The responsibility for termination or change of employment is defined as a separate process.

3.5.3.2 Cloud9 Software's assets should be handed in at the end of the need for the use of these assets.

3.5.3.3 Cloud9 Software should change or terminate access rights at termination or change of employment.

3.5.3.4 Notification on employment termination or change should be carried out through the procedures defined in the human resource system.

3.6 Information security regarding physical conditions

3.6.1 Security areas

3.6.1.1 IT equipment and information that require protection will be placed in secure physical areas. Secure areas have suitable access control to ensure that only Authorised personnel have access. The following zones s be utilised:

Security level	Area	Security
Green	No access restrictions	No access control during ordinary office hours. Internal and sensitive information should not be printed out in this zone.
Yellow	Areas where internal information may be found during office hours. Offices, meeting rooms, some archives, some technical rooms like labs, printer rooms.	All printouts should be protected with "Follow me" function. Access control: Key card
Red	Restricted areas requiring special authorisation . Computer rooms, server rooms, archives, etc. containing sensitive information.	All printouts should be protected with "Follow me" function. Access control: Key card

3.6.1.2 Outside our data centre we have a single office (the technical room) which is currently a restricted area. This is a physically combination lock on the door. Our policy is that only Cloud9 Software staff have access to the combination. Visitors must be accompanied by a member of staff.

3.6.1.3 The IT security manager is responsible for approving physical access to technical room.

3.6.1.4 The Physical security manager is responsible for the approval of physical access to areas other than technical room.

3.6.1.5 All of Cloud9 Software's buildings are secured according their classification by using adequate security systems.

3.6.1.6 Red zones are properly secured against damage caused by fire and water.

3.6.1.7 All external doors and windows must be closed and locked at the end of the work day.

3.6.1.8 Access cards may be supplied to workers, technicians, and others after proper identification

3.6.1.9 Anyone receiving visitors in the yellow zone is responsible for the supervision of their visitors.

3.6.1.10 Visitors in the red zone must be signed in and out and must carry visible guest cards or personal access cards.

3.6.1.11 Visitors in the red zone are escorted

3.6.2 Securing equipment

3.6.2.1 IT equipment classified as "high" is protected against environmental threats (fires, flooding). Classification of equipment should be based on risk assessments.

3.6.2.2 Information classified as "sensitive" must not be stored on portable computer equipment (e.g. laptops, cell phones, memory sticks, etc.). If it is necessary to store this information on portable

equipment, the information must be password protected and encrypted in compliance with guidelines from the IT department.

3.6.2.3 During travel, portable computer equipment should be treated as carry-on luggage.

3.6.2.4 Areas classified as "red" must be secured with suitable fire extinguishing equipment with appropriate alarms.

3.6.2.5 Fire drills are carried out on a regular basis.

3.7 IT Communications and Operations Management

3.7.1 Operational procedures and areas of responsibility

3.7.1.1 Any purchase and installation of IT equipment must be approved by the System Owner.

3.7.1.2 Purchase and installation of software for IT equipment must be approved by the System Owner.

3.7.1.3 The System Owner should ensure documentation of the IT systems according to Cloud9 Software's standards.

3.7.1.4 Changes in System should only be implemented if well-founded from a business and security standpoint.

3.7.1.5 The System Owner should have emergency procedures to minimise the effect of unsuccessful changes to the IT systems.

3.7.1.6 Operational procedures should be documented. Documentation must be updated following all substantial changes.

3.7.1.7 Before a new IT system is put in production, plans and risk assessments are in place to avoid errors. Additionally, routines for monitoring and managing unforeseen problems are in place.

3.7.1.8 Duties and responsibilities should be separated in a manner reducing the possibility of unauthorised or unforeseen abuse of Cloud9 Software's assets.

3.7.1.9 Development, testing and maintenance should be separated from operations to reduce the risk of unauthorised access or changes, and to reduce the risk of error conditions.

3.7.2 Third party services

3.7.2.1 All contracts regarding outsourced IT systems (i.e. Our sub-processors) are GDPR compliant. They are checked annually to be sure they continue to meet the obligations of GDPR.

3.7.3 System planning and acceptance

3.7.3.1 Requirements for information security are taken into consideration when designing, testing, implementing, and upgrading IT systems, as well as during system changes. Processes have been developed for change management and system development/maintenance.

3.7.3.2 IT systems are dimensioned according to capacity requirements. The load is monitored to apply upgrades and adjustments in a timely manner.

3.7.4 Protection against malicious code

3.7.4.1 Computer equipment must be safeguarded against virus and other malicious code. This is the responsibility of the System Administrator.

3.7.5 Backup

3.7.5.1 The System Administrator is responsible for carrying out regular backups and restore of these backups, as well as data storage on Cloud9 Software's IT systems according to their classification.

3.7.5.2 Backups are stored externally in a separate, protected zone.

3.7.6 Network administration

3.7.6.1 The System Administator has the overall responsibility for protecting Cloud9 Software's internal network.

3.7.6.2 All access to Cloud9 Software's networks is logged.

3.7.7 Management of storage media

3.7.7.1 There are procedures in place for the management of removable storage media. Implementation is the responsibility of each employee.

3.7.7.2 Storage media should be disposed of securely and safely when no longer required, using formal procedures.

3.7.8 Exchange of information

3.7.8.1 Procedures and controls have been established for protecting exchange of information with third parties and information transfer. Third party suppliers must comply with these procedures.

3.7.8.2 Cloud9 Software has the right to access personal e-mail and other personal data stored on Cloud9 Software's computer networks in line with relevant national legal requirements

3.7.9 Use of encryption

3.7.9.1 Storage and transfer of sensitive information is encrypted or otherwise protected.

3.7.10 Electronic exchange of information

3.7.10.1 Information exchanged across public networks in connection with e-commerce, is protected against fraud, contractual discrepancies, unauthorised access, and changes.

3.7.10.2 The system owner ensures that publicly accessible information, e.g. on Cloud9 Software's web services, is adequately protected against unauthorised access. Each year a 3rd party completes a formal penetration test. Those tests attempt to gain unauthorised access to our systems. The results are presented back to Cloud9 Software and any threats are mitigated.

3.7.11 Monitoring of system access and usage

3.7.11.1 Access and use of IT systems should be logged and monitored to detect unauthorised information processing activities.

3.7.11.2 Usage and decisions should be traceable to a specific entity, e.g. a person or a specific system.

3.7.11.3 The IT department should register substantial disruptions and irregularities of system operations, along with potential causes of the errors.

3.7.11.4 Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored to ensure reliable operation and availability.

3.7.11.5 The IT department should log security incidents for all essential systems.

3.7.11.6 The IT department should ensure that system clocks are synchronized to the correct time.

3.7.11.7 [Usage of information systems containing personal information may be regulated. Check your local legislation…]

3.8 Access Control

3.8.1 Business requirements

3.8.1.1 Written guidelines for access control and passwords based on business and security requirements should be in place. Guidelines should be re-evaluated on a regular basis.

3.8.1.2 Guidelines should contain password requirements (frequency of change, minimum length, character types which may/must be utilised, etc.) and regulate password storage.

3.8.2 User administration and responsibility

3.8.2.1 Employees accessing systems must be authenticated according to guidelines.

3.8.2.2 Employees should have unique combinations of usernames and passwords.

3.8.2.3 Employees are responsible for any usage of their usernames and passwords. Employees should keep their passwords confidential and not disclose them unless explicitly Authorised by the CSO.

3.8.3 Access control/Authorization

3.8.3.1 Access to information systems should be Authorised by immediate superiors in accordance with the system owner directives. This includes access rights, including accompanying privileges. Authorizations should only be granted on a "need to know" basis and regulated according to role.

3.8.3.2 The immediate superior should alert the system administrator about granting access and changes in accordance with the directives from the system owner.

3.8.3.3 Roles and responsibilities with accompanying access rights should be described based on the following classifications.

- Internal (several roles)
- External (several roles)
- Student
- Public
- Others

3.8.4 Network access control

3.8.4.1 The IT department is responsible for ensuring that network access is granted in accordance with access policy.

3.8.4.2 Employees should only have access to the services they are Authorised for.

3.8.4.3 The access to privileged accounts and sensitive areas should be restricted.

3.8.4.4 Employees should be prevented from accessing unAuthorised information.

3.8.5 Mobile equipment and remote workplaces

3.8.5.1 Remote access to Cloud9 Software's computer equipment and services is only permitted if the security policy has been read and understood and the IT regulations signed.

3.8.5.2 Remote access to Cloud9 Software's network may only take place through security solutions approved by the IT department.

3.8.5.3 Mobile units should be protected using adequate security measures.

3.8.5.4 Information classified as sensitive must be encrypted if stored on portable media, such as memory sticks, PDAs, DVDs and cell phones. [The use of cryptography may be subject to local legislation.]

3.9 Information Systems Acquisition, Development and Maintenance

3.9.1 Security requirements for information systems

3.9.1.1 Definitions of operational requirements for new systems or enhancements to existing systems always contain security requirements.

3.9.2 Cryptographic controls

3.9.2.1 Guidelines for administration and use of encryption for protecting information is in place.

3.9.3 Security of system files

3.9.3.1 All changes to production environments comply with existing processes.

3.9.3.2 The implementation of changes to the production environment is controlled by formal procedures for change management, to minimise the risk of damaged information or information systems.

3.9.4 Security in development and maintenance

3.9.4.1 Systems developed for or by Cloud9 Software satisfy definite security requirements, including data verification, securing the code before being put in production, and use of encryption.

3.9.4.2 All software is thoroughly tested and formally accepted by the system owner before being transferred to the production environment.

3.9.5 Risk assessment

3.9.5.1 Prior to new systems classified as “high”, or substantial changes in systems classified as “high” are put in production, a risk assessment is carried out.

3.10 Information Security Incident Management

3.10.1 Responsibility for reporting

3.10.1.1 All breaches of security, along with the use of information systems contrary to routines, are treated as incidents.

3.10.1.2 All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to management or directly to the CSO.

3.10.2 Measurements

3.10.2.1 Process have been developed for incident management and reporting. The routines contain measures for preventing repetition as well as measures for minimising the damage.

3.10.2.2 The CSO should ensure that process are in place for defining the cost of security incidents.

3.10.3 Collection of evidence

3.10.3.1 The system administrator is familiar with simple routines for collecting evidence.

3.11 Continuity Planning

3.11.1 Continuity plan

3.11.1.1 A plan for continuity and contingencies covering critical and essential information systems and infrastructure has been developed

3.11.1.2 The continuity plan is consistent with Cloud9 Software's overall contingencies and plans.

3.11.1.3 The continuity plan is tested on a regular basis (annually) to ensure adequacy, and to ensure that management and employees understand the implementation.

3.11.1.4 Production systems and other systems classified as "high" have backup solutions.

3.12 Compliance

3.12.1 Compliance with legal requirements

3.12.1.1 Cloud9 Software must comply with current laws, as well as other external guidelines, such as (but not limited to):

- Act relating to working environment, working hours and employment protection
- Regulations relating to systematic health, environmental and safety activities in enterprises
- Act relating to the processing of personal data (GDPR)
- Act relating to annual accounts
- Regulations relating to fire preventing measures and supervision

3.12.2 Safeguarding personal information according to the legal requirements

3.12.2.1 As a data processor we are GDPR Compliant.

With the introduction of new European Union (EU) legislation regarding the collection, storage and processing of personal data, Cloud9 Software (C9S) has been working to ensure that the Intelligentschedule.com service is compliant in advance of its introduction. The General Data Protection Regulation (GDPR) is due for introduction across the EU in May 2018 and places additional obligations on Data Processors of personal data. At Cloud9 Software we take these obligations very seriously. We have produced this short summary paper to outline how we will fulfil our GDPR (as Data Processor) Obligations. Below are the key GDPR obligations for data processors and how C9S fulfils each.

Establish a representative in the EU, if the organisation is not located within the EU (in accordance with Article 27). Because Cloud9 Software Limited is based in Liverpool, United Kingdom, we are not required to nominate a Representative. Our registered address is: 95 South Road [2nd Floor], Waterloo, Liverpool, United Kingdom, L22 0LR.

Only Act on the written instructions of the controller (Article 29). We commit to only complete any data related actions with the written instructions from the nominated key user for each customer account. This instruction will be accepted either electronically (email, helpdesk ticket response) or in written form. If the key user is no longer available at the customer organisation, we provide an offline process for the nomination of a new key user. Please contact support for more information about this process.

Implement and Comply with an Adequate Data Processing Agreement (DPA). C9S has re-worked the terms of service and privacy policy associated with the service and introduced a GDPR compliant data processing agreement (DPA) associated to the terms of service and privacy policy. We explicitly name our sub-data processors. All versions of our terms of service are GDPR compliant from September 2017 onwards. The latest versions can be found here:

- Our terms of service: https://www.intelligentschedule.com/en-gb/terms-and-conditions/
- Our privacy Policy: https://www.intelligentschedule.com/en-gb/privacy-policy/
- Our data processing agreement: https://www.intelligentschedule.com/en-gb/data-processing-agreement/
- Our list of data processors: https://www.intelligentschedule.com/en-gb/sub-processors/

Nominate a data protection officer if required in accordance with Article 37. Cloud9 Software Limited have nominated Paul Darlow (Director) as our Data Protection Officer. He can be contacted by email (paul.darlow@cloud9software.co.uk), by Phone (+44 (0) 151 928 8811) or by writing to: 95 South Road, Waterloo, Liverpool, United Kingdom, L22 0LR

Restrict the appointment of sub-data processors (Article 28.2). We maintain a list of Sub-data processors that support the intelligentschedule.com service. As part of the terms of service, the data processing agreement details the current list of sub-processes. The current list of data sub-processors can be found here: https://www.intelligentschedule.com/en-gb/sub-processors/ If C9S add a new data sub-processor we will notify the key user and the nominated data protection officer (which may be the same person) of each account by email of the details (country of operation, purpose and name of service/organisation) of the new data sub-processor. Each customer has the right to not accept any new data processor and they will be able to terminate their use of the service.

Keep a Record of Processing activities in accordance with Article 30.2. Cloud9 Software are obligated to keep records relating to the processing of data as part of the intelligentschedule.com service. Specifically, we maintain:

- the name and contact details of the key user and the data protection officer for each customer; and
- A list of third countries (i.e. our sub-processor's locations) that personal data may be transferred to

Co-operate with the supervisory Authorities (such as the ICO) in accordance with Article 31. We are committed to fulfilling our data processing obligations under the GDPR rules. As such we commit to cooperate and comply with all instructions issued by a GDPR supervisory authority.

Implement Adequate Data Security in accordance with Article 32. In addition to security processes (both physical and electronic) offered by our hosting partner (Amazon Web Services), Cloud9 Software has active Data Security Policies and Procedures. This includes our Business Continuity Plan. On an annual basis, all key staff are required to undertake Data Security training. As part of this annual session we also take the Opportunity to review the policies and procedures and update them if required. A summary of the current security policies and procedures can be found here: https://support.intelligentschedule.com/solution/articles/22000180240-data-security

Notify personal data Breaches to the Data Controller. For each of our customers we maintain the name of the Key user. In addition, we ask our customers to nominate a data protection officer. This may be the same person. In the event that we become aware of a data breach, we will inform both the nominated key user and data protection officer for each customer. We will communicate by email

detailing the nature of the data breach and, if we are aware, detail the scope of the breach. We will communicate as soon as practically possible. It is the responsibility of our customers to update C9S if the key user or the data protection officer details we hold (including incorrect email addresses) change.

3.12.3 Compliance with security policy

3.12.3.1 All employees must comply with the Information security policy and guidelines. Enforcement is the responsibility of system owner.

3.12.3.2 Employees are aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following court orders.

3.12.4 Controls and audits

3.12.4.1 Audits are planned and arranged with the involved parties to minimise the risk of disturbing the activities of Cloud9 Software.

References

Internal references

Version	Comment	Responsible
1.0	Employee Confidentiality agreement	Paul Darlow
1.0	GDPR Compliance (as a Processor) Overview	Paul Darlow
2.0	Business Continuity Plan	Judy Weeks

External references

[ISO27001] ISO 27001: 2005. Information security – Security techniques – Information security management systems – Requirements**.**

[ISO27002] ISO/IEC 27002: 2005 Information security – Security techniques – Code of practice for information security management.

[ISO27005] ISO/IEC 27005: 2008 Information security – Security techniques – Information security risk management.

[OECD] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. http://www.oecd.org/dataoecd/16/5/15584616.pdf

[BPD107] Power Supply Requirements for ICT Rooms. Best Practice Document. http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs107.pdf

[BPD108] Ventilation and Cooling Requirements for ICT Rooms. Best Practice Document. http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs108.pdf