Assurance | Advisory
Risk | Compliance

ScreenCloud

INDEPENDENT SERVICE AUDITOR'S REPORT SOC 3® AT A SERVICE ORGANIZATION RELEVANT TO SECURITY AND CONFIDENTIALITY

June 1, 2021 through May 31, 2022

Table of Contents

SECTION 1 – INDEPENDENT SERVICE AUDITOR'S REPORT

AARC-360
8000 Avalon Boulevard, Suite 100 Alpharetta, GA 30009
Tel: +1 866 576 4414
www.AARC-360.com

Independent Service Auditor's Report

To: ScreenCloud

Scope

We have examined ScreenCloud's ('ScreenCloud', 'the Company', or 'the Service Organization') accompanying assertion titled "Assertion of ScreenCloud Management" (assertion) that the controls within ScreenCloud's Digital Signage Software services and systems (system) were effective throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that ScreenCloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security and confidentiality (AICPA, Trust Services Criteria).*

ScreenCloud uses various subservice organizations ('the Subservice Organization') to provide cloud hosting and Platform as a Service (PaaS) services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ScreenCloud, to achieve ScreenCloud's service commitments and system requirements based on the applicable trust services criteria. The description presents ScreenCloud's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ScreenCloud's controls. The description does not disclose the actual controls at the Subservice Organization. Our examination did not include the services provided by the Subservice Organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ScreenCloud, to achieve ScreenCloud's service commitments and system requirements based on the applicable trust services criteria. The description presents ScreenCloud's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ScreenCloud's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

ScreenCloud is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ScreenCloud's service commitments and system requirements were achieved. ScreenCloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ScreenCloud is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the Service Organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve ScreenCloud's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ScreenCloud's service commitments and system requirements based the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within ScreenCloud's Digital Signage Software services and systems were effective throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that ScreenCloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

AARC-360

Alpharetta, Georgia
July 12, 2022

SECTION 2 – ASSERTION OF SCREENCLOUD MANAGEMENT

Assertion of ScreenCloud Management

July 12, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within ScreenCloud's ('ScreenCloud', 'the Company', or 'the Service Organization') Digital Signage Software services and systems (system) throughout the period June 1, 2021 through May 31, 2022], to provide reasonable assurance that ScreenCloud's service commitments and system requirements relevant to security and confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

ScreenCloud uses various subservice organizations ('the Subservice Organization') to provide cloud hosting and Platform as a Service (PaaS) services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ScreenCloud, to achieve ScreenCloud's service commitments and system requirements based on the applicable trust services criteria. The description presents ScreenCloud's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ScreenCloud's controls. The description does not disclose the actual controls at the Subservice Organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ScreenCloud, to achieve ScreenCloud's service commitments and system requirements based on the applicable trust services criteria. The description presents ScreenCloud's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ScreenCloud's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that ScreenCloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100*, 2017 Trust Services Criteria for Security and confidentiality (AICPA, Trust Services Criteria)*. ScreenCloud's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 4.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that ScreenCloud's service commitments and system requirements were achieved based on the applicable trust services criteria.

_____

Luke Hubbard
CTO

SECTION 3 - SCREENCLOUD'S DESCRIPTION OF THE BOUNDARIES OF ITS DIGITAL SIGNAGE SOFTWARE SERVICES AND SYSTEMS

ScreenCloud's Description of the Boundaries of its Digital Signage Software services and systems

ScreenCloud's Services Overview

ScreenCloud was founded in 2015, headquartered in London, UK with additional offices in Los Angeles, Belfast, and Bangkok. ScreenCloud is a cloud-based content management software for digital signage networks of any size. It provides a simple and easy-to-use solution that helps businesses transform their spaces and communicate better with customers and employees.

ScreenCloud serves customers in key sectors such as manufacturing, retail, hospitality and retail, events, franchise management, education, fitness and places of worship.

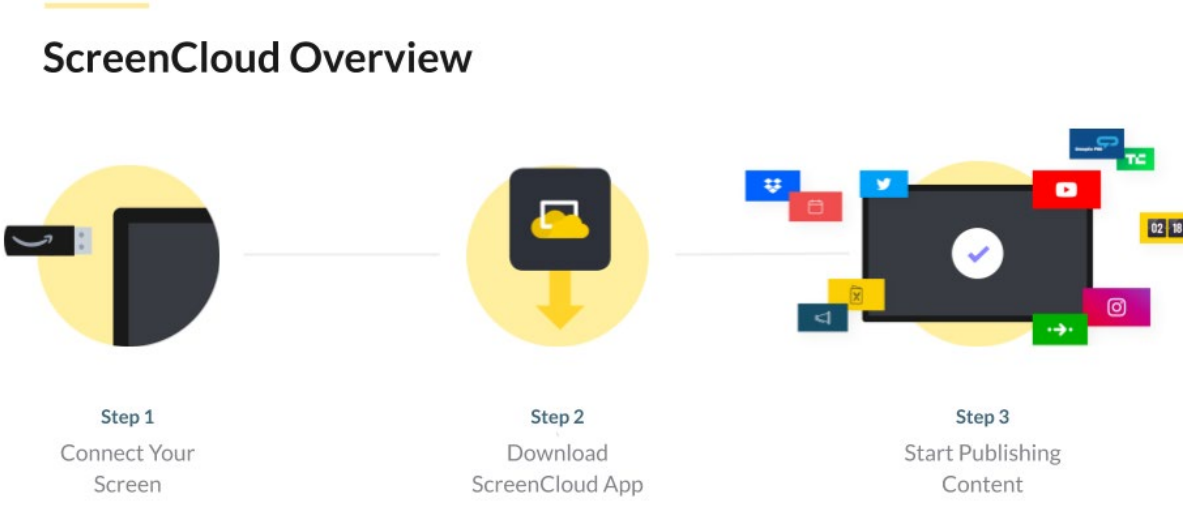
Products and Services

With ScreenCloud, companies can:

- Display, and control, meaningful content on one, or thousands of digital screens anywhere in the world.
- Creatively elevate information. An integrated digital screen experience increases visibility of key messages across entire organisations and key audiences.
- Increase customer and employee attention by displaying important updates, campaigns or product information in an engaging format.
- Digitise traditional communication approaches by providing a modern cloud-based platform to control the screens around them.

ScreenCloud runs on almost any media player which allows customers to turn any screen or device they already have into a digital screen. The focus is on putting the power of the software solution in the hands of communication experts versus the IT department through supporting consumer-grade hardware and providing a simple self-serve experience.

ScreenCloud also specialises in customizable content curation with an eco-system of 80+ apps and integrations, including Slack, Instagram, and CNN for customers to create effective screen content.



Principal Service Commitments and System Requirements

ScreenCloud designs its processes and procedures related to its cloud SaaS service to meet its objectives for its Content and Screen Management services. Those objectives are based on the service commitments that ScreenCloud makes to user entities, the laws and regulations that govern the provision of digital signage cloud services, and the financial, operational, and compliance requirements that ScreenCloud has established for the services. The digital signage content and screen management services of ScreenCloud are subject to the security and privacy requirements of the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which ScreenCloud operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardised and include, but are not limited to, the following:

- Security principles within the fundamental designs of the signage content and screen management service.
- Access considerations that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Ability to integrate major Single Sign-On (SSO) providers.
- Ability to integrate multi-factor authentication techniques in conjunction with your identity providers.
- Code Development quality assurance testing, release and application scanning.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Continuous monitoring of service infrastructure for reliability and security.

ScreenCloud establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ScreenCloud's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organisation-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the systems are operated and monitored, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Content and Screen Management Service.

Components of the System Used to Provide the Services

Infrastructure

The ScreenCloud digital signage service runs on modern elastic, serverless, web application hosting and database platform services provided by Amazon Web Services (AWS). The service is accessible globally via the internet.

Software

The ScreenCloud application is a digital content display application available for the following client platforms: ChromeOS, Android, Amazon FireOS, Windows, MacOS, iOS, LG WebOS and BrightSign. It is developed and maintained by ScreenCloud's in-house software Engineering Team. The software Engineering Team enhances and maintains the client application to provide service for the company's customers. ScreenCloud's client software is available to download from the Apple, Google, Amazon app stores and the ScreenCloud Website.

The client application connects to the ScreenCloud cloud hosted screen management service and receives a configuration of content to display and schedule. The information and content is cached locally on the player device to support off-line service if the players' internet connection is unreliable. The player client software periodically connects to the screen management service to receive content and configuration updates. Information about the players connected to an account, configuration, apps and content being displayed can be retrieved by users through logging into the ScreenCloud management service.

A cloud-based management website provides the ability to register, manage, configure, communicate and deliver content to customer screens.

The ScreenCloud web interface is a multi-user, multi-tenant web-based application that helps to manage the flow of information between the ScreenCloud service and the ScreenCloud player enabled screens on customer premises. The website allows customers to pair devices, manage content, integrate apps, raise support requests, manage their account and retrieve certain audit information.

People

ScreenCloud has a staff of approximately 117 employees organised in the following functional areas:

- *Senior Leadership Team.* Includes the CEO, CFO, CTO, VP of Engineering, VP of People, VP Customer Success, VP of Product, and VP of Marketing. They are responsible for the overall governance of ScreenCloud, formulating its strategy and structure, overseeing company-wide activities, and protection of the company's assets and reputation.
- *Business support*. The Team consists of Cyber Security & IT Operational functions and company administrative support staff, such as finance, people & culture and office management. These people provide support in the day to day running of the company ensuring companywide objectives are met.
- *Engineering*: ScreenCloud's Engineering Team is led by a VP Engineering, who provides strategic direction for the engineering department, and line management to three Director-level Engineers (1 x Engineering Director, 2 x Director of Engineering - one of whom has additional 'Site Lead' responsibility for our Belfast front-end hub). They are responsible for the development of the software as well as making improvements and enhancements to it as per the business needs. Main responsibilities include:
    - Building, testing and deploying code and feature changes
    - Maintaining service availability and configuration management
    - Providing monitoring, scanning and penetration testing
    - Maintaining business continuity disaster recovery capabilities
    - Ensuring a simple and powerful user interface of the product
- *Product.* The ScreenCloud Product Team is responsible for understanding and validating customer requirements, defining feature requests and bringing the product vision to life.
- *Marketing.* Responsible for defining and managing the brand, monitoring and managing social media, producing internal and external communications, educating customers through content and producing marketing and promotional materials.
- *Professional Services.* The professional services department provides ScreenCloud's Enterprise clients bespoke innovative services such as Onboarding, Project Management, content strategy, bespoke application development and account auditing and optimizations.
- *Customer Support.* ScreenCloud has a growing customer support team based in all of our hubs, making sure 24/5 support to customers is provided in a timely and efficient manner. The main goal of the Team is to answer, solve, track and escalate all pre-sales and post-sales questions or problems.
- *Customer Success.* The Customer Success department handles the post-sale relationships with ScreenCloud's existing customers. Focusing on customer adoption, customer advocacy, churn reduction, customer training and proving ROI.
- *Enterprise Account Management*. The Enterprise Account Management team is a commercially focused department which is responsible for developing new business and expansion opportunities from existing customers.

ScreenCloud prides itself on hiring skilled experienced professionals to manage the day to day business operations, product and code development and engineering of customer solutions. Each employee has access to an annually renewed personal development fund to enhance their own capabilities. A collective learning budget is centralised and made available via line management channels of approval. This enables our people to attend more formal career development training to enhance skills and promote the latest methods of working.

Data

Data, as defined by ScreenCloud, constitutes the following:

- Organisational account subscription data
- User account data
- App configuration data
- Player content configuration data
- User uploaded content
- System files
- Error logs

Content processing is initiated by creating or updating the content displayed on an individual or group of players managed by a customer. This request typically comes from a user logged into the Studio content management system (CMS) or an update from a connected app such as Twitter, Facebook or Instagram etc.…

ScreenCloud uses Transport Layer Security to encrypt communication exchanges with CMS users and content delivered to Players running on managed screens.

Processes and Procedures

Management has developed and defined procedures to restrict or control logical access to all layers of the ScreenCloud service. Amendments to these procedures are performed annually and authorised by the Senior Leadership Team. These procedures cover the following key security life cycle areas:

- Data classification and protection (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact and residual risk resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of risk management assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices configuration

SECTION 4 - SCREENCLOUD'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ScreenCloud's Principal Service Commitments and System Requirements

ScreenCloud designs its processes and procedures related to ScreenCloud to meet its objectives for its Digital Signage Software services and systems. Those objectives are based on the service commitments that ScreenCloud makes to user entities, the laws and regulations that govern the provision of Digital Signage Software services and systems and the financial, operational and compliance requirements that ScreenCloud has established for the services. The Digital Signage Software services and systems of ScreenCloud are subject to the security and confidentiality requirements in accordance with client contractual obligations.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Digital Signage Software services and systems that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

ScreenCloud establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ScreenCloud's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Digital Signage Software services and systems.

Complementary Subservice Organisation Controls (CSOCs)

ScreenCloud utilises multiple subservice organisations to perform certain key operating functions for ScreenCloud's platform. The accompanying description of controls includes only those policies, procedures, and controls at ScreenCloud, and does not extend to policies, procedures and controls at the Subservice Organizations.

ScreenCloud uses the following subservice organisations to implement portions of its platform and the following tables present the applicable Trust Services Criteria that are intended to be met by controls at each subservice provider, alone or in combination with controls at ScreenCloud, and the types of controls expected to be implemented at the subservice provider to meet those criteria.

Subservice Organisations

The ScreenCloud platform is built on top of AWS, AWS RDS, Google Cloud Platform, Auth0 (Okta), Filestack, and GitHub cloud hosting and Platform as a Service (PaaS) services. Each subservice organisation undergoes its own audit processes to include an annual AICPA based SOC 2 audit, or equivalent, and is examined annually by ScreenCloud. It is expected that each Subservice Organisation has implemented the following types of controls to support the associated criteria.

No.	Complementary Subservice Organisation Controls (CSOCs)
	Amazon Web Services (AWS)
1.	AWS is responsible for identifying, implementing measures and monitoring to prevent or mitigate threats consistent with the risk assessment.

No.	Complementary Subservice Organisation Controls (CSOCs)
2.	AWS is responsible for restricting logical and physical access to data centre facilities, backup media and other system components including firewalls, routers and servers supporting the AWS managed cloud services.
3.	AWS is responsible for monitoring the integrity and operation of their foundation cloud platform services.
4.	AWS is responsible for the management, review and validation of any third-party vendors with access to the AWS infrastructure and/or facilities.
5	AWS RDS is responsible for maintaining logical segregation from other RDS clients.
6	AWS RDS is responsible for anti-malware security to identify malicious software within system components including firewalls, routers, servers and software.
7	AWS RDS is responsible for monitoring the integrity and operation of their cloud platform service.
8	AWS RDS is responsible for the management, review and validation of any third-party vendors with access to the Citus Data infrastructure and/or facilities.

No.	Complementary Subservice Organisation Controls (CSOCs)
	Auth0 (Okta)
1.	Auth0 is responsible for identifying, implementing measures and monitoring to prevent or mitigate threats consistent with the risk assessment.
2.	Auth0 is responsible for restricting logical and physical access to data centre facilities, backup media and other system components including firewalls, routers and servers supporting the Auth0 managed cloud service.
3.	Auth0 is responsible for maintaining logical segregation from other Auth0 clients.
4.	Auth0 is responsible for anti-malware security to identify malicious software within system components including firewalls, routers, servers and software.
5.	Auth0 is responsible for monitoring the integrity and operation of their cloud platform service.
6.	Auth0 is responsible for the management, review and validation of any third-party vendors with access to the Auth0 infrastructure and/or facilities.

No.	Complementary Subservice Organisation Controls (CSOCs)
	Filestack, ImgX, CloudConvert
1.	Filestack is responsible for identifying, implementing measures and monitoring to prevent or mitigate threats consistent with the risk assessment.
2.	Filestack is responsible for restricting logical and physical access to data centre facilities, backup media and other system components including firewalls, routers and servers supporting the Filestack managed cloud service.
3.	Filestack is responsible for maintaining logical segregation from other Filestack clients.
4.	Filestack is responsible for anti-malware security to identify malicious software within system components including firewalls, routers, servers and software.
5.	Filestack is responsible for monitoring the integrity and operation of their cloud platform service.

No.	Complementary Subservice Organisation Controls (CSOCs)
6.	Filestack is responsible for the management, review and validation of any third-party vendors with access to the Filestack infrastructure and/or facilities.

No.	Complementary Subservice Organisation Controls (CSOCs)
	Google Cloud Platform (GCP)
1.	GCP is responsible for identifying, implementing measures and monitoring to prevent or mitigate threats consistent with the risk assessment.
2.	GCP is responsible for restricting logical and physical access to data centre facilities, backup media and other system components including firewalls, routers and servers supporting the GCP managed cloud services.
3.	GCP is responsible for maintaining logical segregation from other GCP clients.
4.	GCP is responsible for anti-malware security to identify malicious software within system components including firewalls, routers, servers and software.
5.	GCP is responsible for monitoring the integrity and operation of their cloud platform services.
6.	GCP is responsible for the management, review and validation of any third-party vendors with access to the GCP infrastructure and/or facilities.

No.	Complementary Subservice Organisation Controls (CSOCs)
	GitHub
1.	GitHub is responsible for identifying, implementing measures and monitoring to prevent or mitigate threats consistent with the risk assessment.
2.	GitHub is responsible for restricting logical and physical access to data centre facilities, backup media and other system components including firewalls, routers and servers supporting the GitHub managed cloud service.
3.	GitHub is responsible for maintaining logical segregation from other GitHub clients.
4.	GitHub is responsible for anti-malware security to identify malicious software within system components including firewalls, routers, servers and software.
5.	GitHub is responsible for monitoring the integrity and operation of their cloud platform service.
6.	GitHub is responsible for the management, review and validation of any third-party vendors with access to the GitHub infrastructure and/or facilities.

Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary service user entity controls contemplated in the design of ScreenCloud's controls are suitably designed and operating effectively, along with related controls at ScreenCloud. Complementary Service User Entity Controls are specific user controls or issues each ScreenCloud client organisation should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by service user entities, nor do they represent procedures that may be necessary in all circumstances.

1. User entities and sub service organisations are responsible for understanding and complying with their contractual obligations to ScreenCloud.
2. User entities are responsible for notifying ScreenCloud of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of ScreenCloud's services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilise ScreenCloud's services.
6. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorised individuals.
7. User entities are responsible for ensuring that data submitted to ScreenCloud is complete, accurate, and timely.
8. Standards and processes are in place for user entities to follow for security, confidentiality and industry guidelines.
9. User entities are responsible for reporting identified security incidents to ScreenCloud.
10. User entities are responsible for maintaining accurate and up to date contact information for ScreenCloud's use.
11. User entities are responsible for maintaining accurate display records used with the ScreenCloud provided service.
12. User entities are responsible for deploying local antivirus protection for owned devices used with the ScreenCloud provided service.
13. User entities are responsible for reporting service failure to the ScreenCloud service support desk.
14. User entities are responsible for ensuring the correct and legal use of data displayed on the ScreenCloud service.
15. User entities are responsible for monitoring ScreenCloud Service Status pages for up to date service availability and defined maintenance periods @ https://status.screencloud.com/