

<b>Policy title:</b>	Guest User Access & Authentication Policy	<b>Updated:</b>	Q4 2022
<b>Policy Family:</b>	Information Security Policies	<b>Affected parties:</b>	Guest users

**Definitions:**

<b>Acceptable Use Policy</b>	The Company's policy (incorporating Password Policy) which authorises usage of, and access to, its Product. This policy forms part of the Company's Information Security policies.
<b>Antivirus Software</b>	Application used to protect a computer from viruses, typically through real time defences and periodic scanning to cover threats, including Trojans, spyware, and other malware.
<b>Authentication</b>	Security method used to verify the identity of a user and authorize access to the Product.
<b>Client</b>	Customers of the Company, including their staff, assets and premises.
<b>Client Account</b>	A valid subscription to the Cognition World Product which allows access to all the Client data.
<b>Company</b>	Cognition Services Ltd (trading as Cognition World)
<b>Encryption</b>	Process of encoding data with an algorithm so that it is unintelligible without the key, used to protect data during transmission or while stored.
<b>Guest User</b>	An individual, identified and authorised by the Client, who is provided with a unique log-in to access and view data within a Client Account
<b>Guest User Access</b>	Authenticated access of a Guest User who is provided with a time-restricted log-in to use the Product and view data belonging to the Client and/or a Client Account.
<b>Guest User Organisation</b>	The organisation where the Guest User is employed.
<b>Password</b>	Sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.
<b>Product</b>	A subscription to the Cognition World analytics platform including all support, software, connectivity, and hardware provision.

**1.0 Overview:** A Client may request that a third party be provided with Guest User Access to a Client Account. This policy is required to protect the data, software and IP of the Company and so this policy forms part of its critical information security. This *Guest User Access and Authentication Policy* reduces any risk of a security incident by requiring consistent application of authentication and access standards. These requirements must be understood and agreed to by the Guest User to receive Guest User Access and to maintain ongoing access to the Product. This policy may be required to protect third-party agreements or regulation in the jurisdictions where the Company operates.

**2.0 Purpose:** This policy:

- Ensures consistent standards are in place for the Authentication of Guest User Access.
- Describes how a Guest User is given the appropriate level of Guest User Access.
- Describes how a Guest User should access the Product.
- Clarifies how Guest User Access complies with policies and standards of the Company.
- Specifies authentication standards and what constitutes appropriate use for a Guest User.
- Explains the right to refuse requests or limit access to a Guest User accessing the Product as the access has the ability to affect the security of both Client Account and/or Company data.

**3.0 Scope:** This policy covers:

- All third parties, contractors, consultants, advisors and anyone identified by the Client as requiring Guest User Access to a Client Account.
- A Guest User who requires access to the Client Account.
- A Guest User who already has been granted Guest User Access to the Client Account.
- The Individual within the Client who authorises Guest User Access on behalf of the Client ("Authoriser")
- The Guest User Organisation which authorises the Guest User to represent it or access the Client Account on its behalf.

## **4.0 Policy**

### **4.1 Account Setup & Authentication:** The following applies in order to provide Guest User Access to a Client Account:

- a) Permission from the Client is required in writing before the Company will allow Guest Access to a Client Account.

<b>Policy title:</b>	Guest User Access & Authentication Policy	<b>Updated:</b>	Q4 2022
<b>Policy Family:</b>	Information Security Policies	<b>Affected parties:</b>	Guest users

- b) Guest Users shall only be granted Guest User Access if they accept the Acceptable Use Policy of the Company.
- c) Guest Users are only granted Guest User Access for the term of the Client Account.
- d) Guest Users shall only be granted the level of access required to perform their function. This shall be determined at the discretion of the Company, unless explicitly specified by the Client.
- e) Guest User Access is provided to an individual Guest User, acting as an agent of the Guest User Organisation.
- f) The Company reserves the right to refuse to provide Guest User Access for a Client Account.

#### **4.2 Account Use:** The following usage requirements apply to the Guest User for Guest User Access:

- a) Guest User Access to the Product and use of the data is bound by the Company's Terms & Conditions
- b) Guest User has no ownership rights to the data. Data ownership rests solely with the Client.
- c) Guest User is only allowed access to data matching the sharing criteria determined by the Company, or if specified by the Client.
- d) Account sharing is strictly not permitted. Guest User Access is provided on this basis only.
- e) Guest User shall never be given administrator access to a Client Account.
- f) Guest User must only access areas of the Product essential to the needs of the Guest User to perform their function.
- g) Should the Guest User knowingly access data outside of their authorisation level they should delete any record(s) of the data and contact the Company immediately.

#### **4.3 Data access and Interpretation**

- a) Guest User is not permitted to re-use or re-publish the data or analytics without the express permission of the Client and/or the Company.
- b) Any views or opinions formed on the data must only be made in consultation with the client. Contextualisation of the data is at the discretion of the Client who have the right to refuse to cooperate.
- c) The Company is not responsible for any losses, exposure or misinterpretation of the data due to access from unauthorised users caused by the loss, theft or mis-use of the authentication details of the Guest User.
- d) Guest User must have appropriate Antivirus Software in place when accessing the Product.

#### **4.4 Use of Passwords**

- a) When accessing the Product, the Guest User must use an acceptable means of authentication.
- b) Passwords must conform to the requirements set out in the Company's Acceptable Use Policy.
- c) If the Guest User has lost their password, they should contact the Company immediately.
- d) Screensaver and other access passwords must be activated immediately after inactivity by the Guest User in order to remove the opportunity for a malicious actor to have unwarranted access.

#### **4.5 Failed Logons** The Company has the right to lock or restrict Guest User Access after three failed logons in order to avoid attempts to 'crack' a password and surreptitiously access a Client Account.

#### **4.4 Account Termination**

- a) If the term of Guest User Access has expired, the Guest User will need to re-apply to the Company for Guest User Access.
- b) If the Client wishes to terminate Guest User Access, the Authoriser or a representative of the Client must immediately convey such a change in circumstances to the Company.
- c) If the Guest User has left the Guest User Organisation, the Client must immediately convey such change in circumstances to the Company.
- d) If a Guest User doesn't require access anymore, the Guest User must immediately convey such change in circumstances to the Company.
- e) At which point the Company has been notified of an intention to terminate, Guest User Access will

<b>Policy title:</b>	Guest User Access & Authentication Policy	<b>Updated:</b>	Q4 2022
<b>Policy Family:</b>	Information Security Policies	<b>Affected parties:</b>	Guest users

be terminated within 48 hours of a working week.

- f) The Company reserves the right to revoke Guest User Access at any time.

**4.5 Applicability of Other Policies** This document is part of the Company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

**5.0 Enforcement** This policy will be enforced by the Directors at the Company. Violation of this policy may result in action including restriction of access or where more serious violations have occurred, the company may report such activities to the applicable authorities.