Access Intelligence Business Continuity Management Policy

1.0 *Policy Objectives*

- To ensure that Access Intelligence has a robust Business Continuity Plan in place. By a process of risk assessment, this shall identify and control those risks which Access Intelligence considers having the potential to cause unplanned interruptions to normal operations and/or the provision of normal service levels to external client and stakeholders.

- To ensure that Access Intelligence has, as an integrated element of the Business Continuity Plan, a comprehensive Disaster Recovery capability. Such capability shall be appropriate to restore normal operations and service in the event of an unplanned interruption being experienced.

- To ensure that Access Intelligence undertakes regular reviews and tests of its Business Continuity and Disaster Recovery Plans to ensure they remain relevant, functional and effective.

- To ensure that Access Intelligence stakeholders, employees, clients and suppliers understand the business benefit of undertaking Business Continuity Management activities, and the roles that they need to undertake to ensure it remains capable of protecting the business.

2.0 *Policy Scope*

Access Intelligence Business Continuity Management Policy shall include the following:

- The entire Company, its subsidiaries, offices and employees

- The following resource types:
  - People
  - Premises
  - Technology
  - Information
  - Suppliers and Partners

3.0 ***Policy Statements***

Access Intelligence shall ensure it has a Business Continuity Management capability which:

- Safeguards the lives, health and welfare of its employees and any other persons involved with the delivery of Access Intelligence operations or the delivery of services to clients.

- Safeguards Access Intelligence's property and assets (including information assets) and including any non-Access Intelligence property and assets (including information) entrusted to Access Intelligence under a contractual agreement which specifically requires such safeguards to be in place.

- Aligns and complies with the requirements of identified applicable legislation and regulations, and any contractual requirements that have been agreed with Access Intelligence's clients.

- Undertakes a "Business Impact Analysis" of the threats and vulnerabilities to the locations, activities and resources defined within the Scope of this Policy.

- Proposes, implements and manages appropriate controls to ensure that any identified threats and vulnerabilities shall be prevented from causing interruptions to Access Intelligence's business.

- Includes an effective disaster recovery capability, which shall be available to address any interruptions that do occur, and which provide a process for returning to normal operations as quickly and safely as possible.

- Includes a formal programme of training and awareness, to ensure that all employees and any other persons included in the Scope of this Policy understand this Policy, related documentation, and their role in the delivery of Access Intelligence's business continuity capability.

- Provides for frequent testing of Access Intelligence's business continuity arrangements and emergency recovery plans and allows for feedback and corrective actions to be incorporated where deficiencies or improvement opportunities are identified during tests.

4.0 *Service Recovery Concepts*

Risks may include natural or man-made disasters.

Examples of risk include:

- Natural disasters – extreme weather, fire, flood, earthquake etc.
- Criminal activity or terrorism
- Public health
- Misuse of information systems, or cyber-attacks.
- Loss of data
- Loss of critical infrastructure or services – power, communications, datacentre etc.
- Human error – e.g. mistakes in operation and maintenance of systems

A full list of all the possible risks is very long. However, it's not necessary to consider an exhaustive list because the consequences are often similar. For the purposes of business continuity planning, Access Intelligence consider the following consequences:

- Services of key suppliers might be disrupted
- Staff might become unavailable for work
- Office environment may become inaccessible or unproductive
- Hosted software systems may become disrupted

4.1 Supplier service disruption

- Critical suppliers should have their own Business Continuity plans. Access Intelligence can choose to rely on them, and wait for recovery.
- Where the supplied service is a commodity service it can make sense to prepare alternative supplier lists, to support substitution in case of major failure.
- Implementing redundancy in supply chains, can be an effective means to ensure continuity of service with least disruption. e.g. dual communications links for internet and telecoms to office.
- Our Risk Assessment activities for Business Processes, and Data Assets, considers the risk to the business of loss of integrity, or availability of the service – this will help to identify the critical supplier list.
- Our Supplier Management activities for critical suppliers considers the state of BC planning within our critical suppliers list.

4.2 Staff availability disruption

- Try to avoid 'key-person dependency' as this creates operational challenges when that person is not available to work. Various strategies can help with this:
    - Identify critical knowledge, and skills related to critical business processes.

- Elicit critical knowledge, in order to create training materials and share with others.
- Identify critical skills, and identify individuals suitable as back-up.
- Identify sources for step-in alternatives for key roles, e.g. through hiring of short-term contractors.

4.3 Office disruption

- Remote working enables staff to continue to work from alternate locations in the case that the office is not accessible, or not a productive environment.
  - The remote environment could be any alternate location with appropriate resources – employee home, or co-working space, or temporary hired office space.
- IT equipment and resources should be designed with remote working capability in mind.
  - Key systems must be available on-line, and should not themselves be dependent on the office environment.
  - Staff should have access to mobile devices.
  - Telephone systems must have capability for re-routing.
  - Information Security controls must be designed to be effective for remote working practices.
- Communications tools and practises should be established that support remote collaboration, and remotes monitoring of key activities.
- Emergency communications strategies must be defined so that it is possible to reach all staff to notify of office disruption in a timely manner.

4.4 Hosted platform disruption

- Hosted platforms providing services to clients must be recoverable. Recovery might be in the same location, or an alternate location.
- Platform 'Disaster Recovery Plans' should be created and tested detailing the technical steps to be enacted.

5.0 ***Responsibilities***

- Senior Management shall define and approve the Business Continuity Strategy; define the scope of this policy and establish and test a full Business Continuity Plan. In the event of a Business Continuity invocation executive management will take control of

the execution of the Business Continuity Plan or Disaster Recovery Activities in order to protect Access Intelligence in line with the policy statements above.

- The Information Security Manager shall be responsible for:
  - Developing Business Continuity Plans in accordance with the direction provided by the Board of Directors, and act as the formal communication route to and from them for all matters relating to business continuity and disaster recovery.
  - Ensuring that location, activity and resource owners within Access Intelligence have delivered upon their requirements (see below).
  - Ensuring that Business Continuity Plans (including disaster recovery options) are regularly reviewed, tested and audited, and that any identified corrective actions or improvement opportunities are promptly identified, addressed and resolved.
  - Providing a programme of training and awareness to Access Intelligence employees.
  - Ensure that all plans associated with Business Continuity include appropriate consideration of Information Security, and that the ISMS will continue to function in the event of a Business Continuity event.

- Location, Activity and Resource Owners shall be responsible for:
  - By risk assessment, identifying the vulnerabilities and threats which may affect the normal operation or service provision of their specific location/activity/resource.
  - Undertaking a Business Impact Analysis and use the results to implement appropriate and effective controls to address the identified threats and vulnerabilities, and regularly reviewing the ongoing effectiveness of these.
  - Creating a detailed disaster recovery response which aims to restore normal operations or operational service levels within an acceptable timeframe in the event of a business interruption being experienced by Access Intelligence or part thereof.
  - Participating in reviews, tests and audits as required by Access Intelligence, and for implementing any corrective actions or improvement opportunities identified.

- The Supplier Managers shall:
  - Ensure that Access Intelligence understands the resilience of its supply chain by requesting and reviewing details of supplier business continuity plans as part of normal supplier assessment activities.
  - Ensure that Access Intelligence has alternative procurement options available should a supplier be unable to continue with normal supply activities due to them being affected by an unplanned business interruption.

- All Access Intelligence employees shall:
  - Attend training provided by Access Intelligence on matters relating to business continuity and disaster recovery.
  - Understand their individual responsibilities (as appropriate to their level and role within the organisation) in ensuring the successful operation of business continuity activities within Access Intelligence.
  - Understand their individual responsibilities (as appropriate to their level and role within the organisation) in implementing a disaster recovery response in the event of a business interruption being experienced by Access Intelligence.

All individuals specified within the scope of this Business Continuity Management Policy (see Section 2.0) shall have individual responsibility for complying with every aspect of this policy. The requirement to comply with Access Intelligence policies is included within the Terms and Conditions of Employment and is noted within each individual user's job description. Any failure to adhere to the requirements of this policy shall result in disciplinary action being taken.

6.0 Document Version Control

This policy needs to be reviewed annually as an absolute minimum, or if required changes ae identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this policy, for example because of a reported information security incident, formal review or audit finding.
- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document.
- A change in the way in which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below:

Version History

Revision	Author	Date	Reason for issue
1.0	Andy Olliver	18/12/2019	Office location has changed, ISO 27001:2013 needs to be achieved
2.0	Adam Palmer	19/01/2021	ISO 27001:2013 was achieved in June 2020
3.0	Adam Palmer	30/03/2021	Service Recovery Concepts

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		21/01/2020
Mark Fautley	Chief Financial Officer		20/01/2021
Mark Fautley	**Chief Financial Officer**		**25/07/2021**