Digital Incident Management Policy

1 Policy Statement

Language Reach will ensure that it manages appropriately any actual or suspected incidents relating to information systems and information within the custody of the Company.

2 Purpose

The aim of this policy is to ensure that Language Reach manages appropriately any actual or suspected security incidents relating to information systems and data.

3 Scope

This document applies to all stakeholders who use Language Reach services and facilities, or have access to, or custody of, customer information or Language Reach information.

All users **must** understand and adopt this policy and are responsible for ensuring the safety and security of the Companies systems and the information that they use or manipulate. This includes both data stored electronically and in any other form.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

4 Definition

This policy needs to be applied as soon as information systems or data are suspected to be or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.

- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Companies knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

5 Risks

Language Reach recognises that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up consistently and correctly.
- To help identify and deal with areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the Company and may result in financial loss and an inability to provide necessary services to our customers.

6 Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Language Reach Security Group. The group enables the Language Reach Information Communications and Telecommunications (ICT) Department to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the Language Reach ICT Department to gain as much information as possible from the business users to identify if an incident has taken place or is occurring.

For full details of the procedure for incident handling please refer to Appendix 3.

7 Policy Compliance

This policy applies to all CYC employees, elected members and any other users of CYC ICT systems. If any user is found to have breached this policy, they may be subject to Language Reach disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

For members this policy will be enforced through Language Reach 's Code of Conduct for elected members.

In such cases the Director of Resources in conjunction with the Head of ICT will manage abuse of this policy by undertaking a documented review with the elected member

involved. The review will be recorded, and the documents will be retained within the centrally held register.
Two incidents of abuse relating to breaches of this policy within a two-year period for the same elected member could constitute a serious abuse and this trigger point would be reported as outlined below.

If you do not understand the implications of this policy or how it may apply to you, seek advice from Language Reach Customer Services Team on tel. +44 (0) 208 677 3775.

8 Policy Governance

The following table identifies who within Language Reach is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of ICT
Accountable	Director of Resources (Section 151 Officer)
Consulted	Language Reach IT Technical Design Authority, Language Reach IT Security Group, Officer Governance Group, Human Resources, Union
Informed	All employees, subcontractors and stakeholders

9 Review and Revision

This policy, and all related appendices, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Service Delivery Manager.

10 References

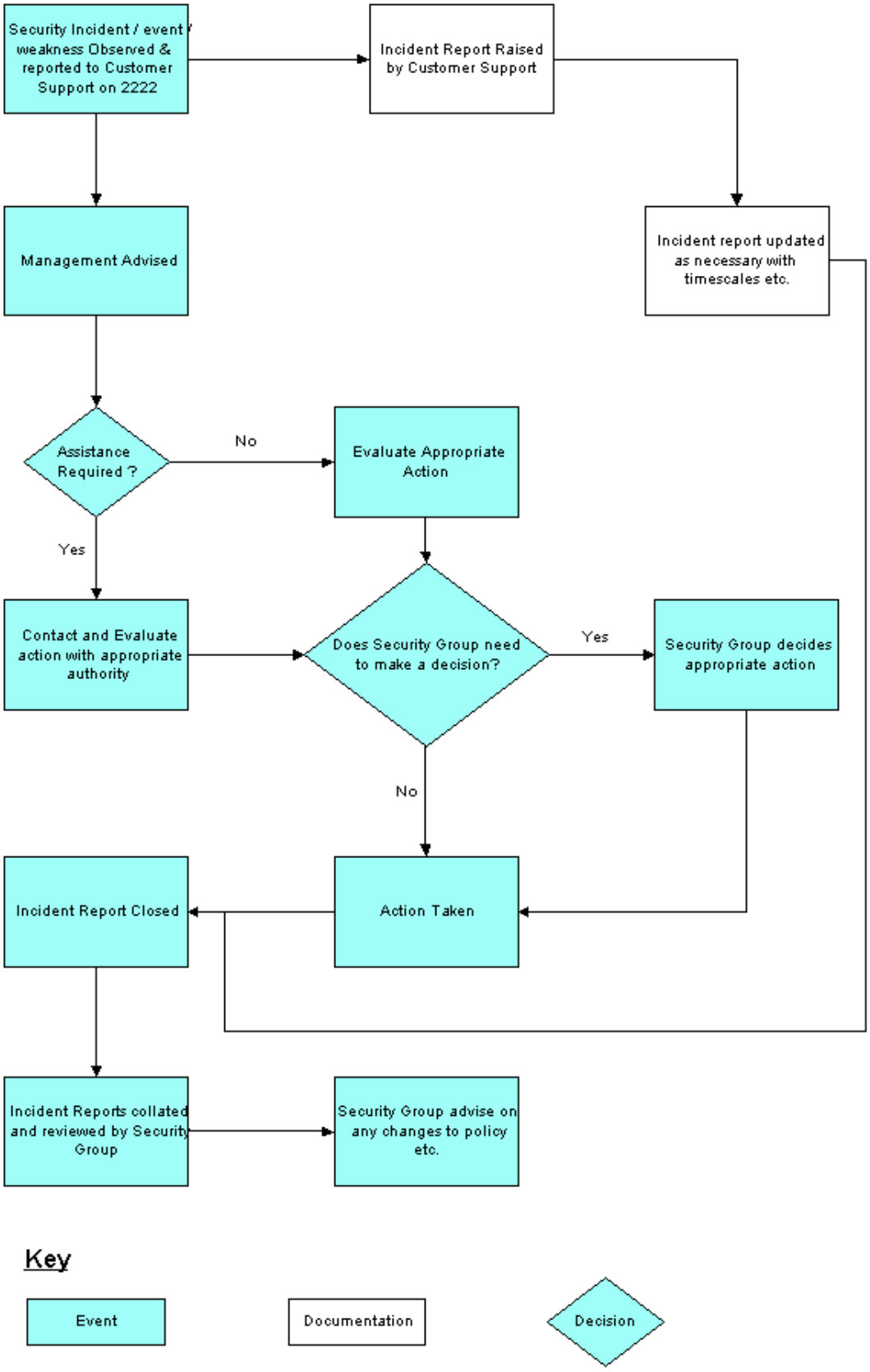
This policy should be read in conjunction with all other Language Reach policy documents and legal documents including the Electronic Communications Policy

11 Key Messages

- All staff should report any incidents or suspected incidents immediately by calling the ITT Customer Services Team on Tel (55)2222 immediately.
- We can maintain your anonymity when reporting an incident if you wish.

- If you are unsure of anything in this policy, you should ask advice from ICT Customer Services Team

12 Appendix 1 – **Process** Flow; Reporting an Information Security Event or Weakness



13 Appendix 2 – Examples of Information Security Incidents and Events

Examples of the most common Information Security Incidents and events are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- None reporting of the receipt of unsolicited mail of an offensive nature.
- None reporting of the receipt of unsolicited mail which requires you to enter personal data.
- Changing data that has been done by an unauthorised person.
- Forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others. (Chain letters can be disturbing to those who receive them by implying bad luck if it is not forwarded for example. These are in fact just either at best a piece of fun which clogs up corporate and international email services wasting resource and at worse an attempt to harvest information from the recipient's machine including contacts information, details of corporate firewalls etc. They should be deleted straight away and not forwarded anywhere.)
- Unknown people asking for information which could gain them access to data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on Language Reach equipment.
- Accessing a computer or database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any Language Reach computer equipment.

This policy will be enforced through the use of the Language Reach 's disciplinary procedures.

Allegations of malicious or misuse will be investigated, and action taken in accordance with Language Reach 's disciplinary procedure. The level of action taken in response to any breach will be dependent on the nature and the findings of any investigation of suspected breaches.

Any suspected breaches of this policy will be managed by the local line manager with assistance from ICT and Human Resources and in accordance with Language Reach 's disciplinary procedures.

14 Appendix 3 - Procedure for Incident Handling

14.1 Reporting Information Security Events or Weaknesses

The following sections detail how users and IT Customer Services Staff must report information security events or weaknesses. Appendix 1 provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

14.1.1 Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from IT Customer Services Staff).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management and either the Information Governance Officer (Veritau Limited) or Caldecott Guardian for the impact to be assessed.

The ITT Customer Services Team will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and contact number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

14.1.2 Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

14.1.3 Reporting Information Security Events and Weaknesses for IT Support Staff

Information security events and weaknesses must be reported to ICT Customer Services who must immediately inform the Business and Customer Services Manager or his

representative as quickly as possible and the incident response and escalation procedure must be followed.

Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Non-compliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human errors.

Should an appropriate response not be received by the person in ICT Customer Services who owns the logged call within 30 minutes the incident / event must be escalated to the Head of ICT.

Incidents must be reported to the ICT Security Group and the Head of IT&T should the incident become service affecting.

A GovCert Incident report (see appendix 5) must be completed by the incident owner for all incident and passed to the ICT Service Delivery Manager.

14.2 Management of Information Security Incidents and Improvements

A consistent approach to dealing with all security events must be maintained across the Company The events must be analysed and the ICT Security Group must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Company on continuing operation during the incident.

All high and medium incidents should be reported to the ICT Security Group. All low incidents should be reported to the Customer Services Team Leader. To decide what level of impact an incident has users should refer to the Risk Impact Matrix in Appendix 4.

14.2.1 Collection of Evidence

If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact ICT Customer Services on (55)2222 for advice.

14.2.2 Responsibilities and Procedures

Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. The ICT Security Group must decide when events are classified as an incident and determine the most appropriate response.

An incident management process must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the Company to those affected.

The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

The actions required to recover from the security incident must be under formal control. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

The officer responsible for an incident / event should risk assess the incident / event based on the Risk Impact Matrix (please refer to Appendix 4). If the impact is deemed to be high or medium this should be reported immediately to ICT Security Group and the Head of IT&T or their representatives.

14.2.3 Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the ICT Security Group and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.