Cyber Security Incident Response Plan Policy

1. Introduction

The purpose of the Cyber Security Incident Response Management Policy is to enable a response to a major incident or disaster by implementing a plan to restore the critical business functions of Deafblind Scotland. To implement a sound policy and procedure to mitigate/early detection of security incidents and actions to be taken to reduce such risks. To ensure all employees of Deafblind Scotland are aware, and kept up to date with regard to the procedures responding to a major cyber breach within the organisation. The Cyber Security Incident Response Policy will assist in maintaining systems at operational level.

2. Managers are responsible for ensuring adherence to the Incident Response Policy within their Departments, overseen by the Chief Executive.

Deafblind Scotland Chief Executive and Senior Management shall ensure that:-

- Incidents are detected as soon as possible and properly reported to external IT Consultants for action and are dealt with in a timely manner in line with external IT Consultants, whereby they will assess, gather all key facts and evaluate the severity of the incident.
- Incidents are handled by appropriate personnel.
- Incidents are properly recorded and documented. (Appendix 1) Incident Reporting Form.
- All employees should report to their Line Managers any data breaches, incidents to the organisation as soon as possible.
- Evidence is gathered, recorded for internal and external scrutiny
- Full extent and implications relating to any incident are risk assessed to ensure negative exposure on the organisation and reputation are minimised.
- Chief Executive, Senior Management will ensure immediate steps are taken to limit ongoing damage, restore affected systems and services to normal operations in line with external IT Consultants advice.
- Escalating serious incidents to Chief Executive, Senior Management
- Ensuring the incident is communicated appropriately with all employees, other businesses, and stakeholders.
- Central point of co-ordination to ensure all findings are correlated and actions are planned.

Consideration should be given to the scale of the problem arising, ie identifying, containment, eradication and recovery of any incident.

- Identifying the severity of any incident.
- Confidentiality – Has sensitive data been accessed, leaked or stolen.
- Integrity – have any systems been altered due to cyber breach.
- Severity – are over 80% of staff unable to work, systems offline with no known resolution. Financial impact on the organisation, reputational damage.
- Evaluating is required regarding any incident and the rated severity of the incident. High, Medium loss risk to Deafblind Scotland.
- Categorisation of any incident for example - Malicious code – Infection to the network. Phishing – Emails attempts to convince someone to trust a link/attachment. Unauthorised Access – Access to systems, accounts, data by an authorised person. Insider – Malicious or accidental action by an employee causing a security incident.

To enable containment, continuity of business requirements and restoring and securing all systems as soon as is practicable, further monitoring and assessment of the incident will be undertaken by the Chief Executive, Board of Directors to identify what has worked and what further processes will require improvement within the organisation.