Information Security Policy

TABLE OF CONTENTS

1 PURPOSE

The purpose of this policy is to define information security as a business process and information as a valuable asset of the business. This policy establishes the baseline levels of security to ensure confidentiality, integrity and availability of INTRAC's information assets.

INTRAC operates through a network of staff and associates. Whilst operations are based in the UK we undertake assignments around the world, involving travel to often remote locations. Access to the internet can be limited in some locations meaning that it may be necessary to temporarily hold some data assets remotely from central servers. This raises particular challenges around ensuring security of data assets. Following the processes outlined in this policy should reduce the risks arising from the challenges of working remotely from INTRAC's head office.

1.1 Related Policies and Notices

This document should be read in conjunction with INTRAC's Data Protection Policy and INTRACs Privacy Notices relating to employees, recruitment, and training applicants on our web pages.

Details of what data resources we hold, how they are used and where they are stored can be found in INTRAC's Data Resource Register. This register is an internal resource. This link is only available internally to INTRAC staff

2 ISSUING AUTHORITY

INTRAC Chair via INTRAC Chief Executive.

3 SCOPE

This policy is applicable to all INTRAC employees, contractors, volunteers, interns and business partners. It addresses all information including but not limited to:

- Electronic data
- Voice
- Image
- Paper

4 POLICY

This policy has several main sections, and within each will be the policy statements, and threats/issues being addressed by that section.

4.1 General Information Security Policy

Information is a vital INTRAC asset. As each employee and contractor, is responsible for the processing and storage of information, each is also the owner of a significant portion of the information assets owned by the INTRAC. INTRAC relies upon each individual to preserve and protect those assets in a consistent and reliable manner. Security controls provide the necessary physical and procedural safeguards to accomplish those goals.

All information, regardless of the form or format, which is created or used in support of INTRAC business activities, is corporate information. Corporate information is a Company asset and must be protected. It must be maintained in a secure, accurate, and reliable manner, and be readily available for authorized use. Information will be classified based on its value to the organization, sensitivity or confidentiality, and legal and/or retention requirements (refer to INTRAC's Data Protection Policy for additional details).

The purpose of information security is to protect information against accidental or malicious disclosure, modification, or destruction. Information will be protected based on its value, confidentiality, and/or sensitivity to INTRAC and the risk of loss or compromise. Information security management enables information to be shared while ensuring protection of that information and its associated computer assets. INTRAC management is responsible for ensuring appropriate controls are in place to preserve the security objectives of confidentiality, integrity, and availability for INTRAC's information assets.

4.1.1 THREATS/ISSUES ADDRESSED

This policy addresses the security issues of confidentiality, data integrity and availability. The disclosure, destruction or prolonged unavailability of Company information could harm the company legally, cause financial loss, or negatively impact the Company's image or competitive advantage. Examples would include

- disclosure of personal data in breach of GDPR or contractual obligations (see INTRAC Data Protection Policy for further information), leading to fines
- disclosure of sensitive management information could negatively impact on INTRAC's image and competitive position
- loss of intellectual property would negatively impact on INTRAC's competitive position

4.2 Individual Use

Individual accountability is required on all INTRAC computer systems. Access to INTRAC computer systems and networks is provided through the use of individually assigned unique computer identifiers, known as user-IDs. Each individual who uses INTRAC computer resources will access resources to which they are authorized by means of their user-ID. Associated with each user-ID is a password which is used to authenticate the person accessing the system or network. Passwords shall be treated as confidential information, and must not be disclosed. All individuals are responsible for all activity performed under their user-ID.

4.2.1 THREATS/ISSUES ADDRESSED

Without accountability, there can be no security. Requiring each individual to sign on using a unique user-ID, activity can be more easily monitored. This auditability provides management with information regarding who performed what activity on what information. It can be used to help resolve system or network problems by providing more complete information, and in conjunction with other polices, remove any expectation of privacy such as with E-mail systems.

Appropriate access control to protected resources can be more easily accomplished through the use of user-IDs, and grouping them according to some like characteristic such as job function, or department, and granting access to the group. This enhances information confidentiality and integrity by ensuring only authorized individuals have the appropriate access to protected resources.

4.3 Confidentiality/Integrity

All INTRAC information will be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. The information owner will classify and secure information within his/her jurisdiction based on the information's value, sensitivity to disclosure, risk of loss or compromise, and ease of recovery. The results of this classification will be recorded centrally in INTRAC's Data Resource Register.

Careful attention must be paid to clauses relating to Intellectual Property (IP) appearing in contracts with clients to ensure that rights to IP, particularly background IP (eg pre-existing materials) are appropriately protected. If not using INTRAC's standard contract template, clauses should be checked with INTRAC's Business Development Manager or another member of SMT before the contract is signed.

4.3.1 THREATS/ISSUES ADDRESSED

Depending on the data, the unauthorized disclosure of sensitive or confidential information could:

- cause the Company to lose its competitive advantage through disclosure of trade secrets, technologies and processes used to conduct business, upcoming marketing events, etc.,
- cause harm to an individual, eg if sensitive or confidential personal data is accessed and misused, eg banking details, credit card numbers,
- cause employee embarrassment if employee personnel or medical data is disclosed,
- result in reputational damage and affect our on-going viability if the data is sensitive
- result in considerable disruption if the breach is reportable under the GDPR (reporting and dealing with ICO investigations),

The unauthorized modification of company information could:

- cause financial statements to be misrepresented,
- corrupt software so that computer systems give unreliable data or fail completely

4.4 Access Control

Physical and logical access control mechanisms will be put in place to ensure information assets are protected commensurate with the value, confidentiality, risk of loss or compromise, or ease of recovery of the information. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). These access privileges should be in accordance with the user's job responsibilities.

Details of logical Access Controls will be recorded centrally in INTRAC's Data Resource Register.

Physical servers will be maintained in secure locations with appropriate physical access controls, as advised by our outsourced IT support function. Cloud based solutions will only be used where we are satisfied that the service provider has suitable security measures in place to restrict access.

Hard copy data resources will be kept in secure locations with appropriate physical access controls, eg locked cabinets with authorised key holders.

Laptops used by staff will require passwords for access and drives will be encrypted. Any portable storage media will also be encrypted and password controlled. Laptops must not be left unattended whilst travelling or in use outside the office.

Remote access to servers will use a VPN that includes encryption and authentication. This may mean that access to servers is not possible over some public networks.

4.4.1 THREATS/ISSUES ADDRESSED

Access control mechanisms ensure that only authorized individuals have the appropriate access to protected resources. Access control mechanisms and processes help ensure the confidentiality, integrity, and availability of information. Without proper access control mechanisms and individual accountability, all information assets are at risk of compromise or loss. Access control processes and mechanisms ensures a level of security is implemented commensurate with risk associated with information asset.

Proper physical security helps ensure the overall security of the protected resource. Unauthorized access to servers could cause the systems to be compromised or taken out of service at the most

inconvenient times. This could cause disruption or stoppage of normal business activities for an extended period of time.

The use of encrypted media (lap-tops, memory sticks etc) for storage removes the need to report such losses to the ICO (Information Commissioner's Office) if the media contained personal data as encryption means that the data is effectively not readable so the risk to the persons concerned is negligible. Without this there could be considerable disruption from an ICO investigation as well as financial loss from the imposition of fines.

4.5 Copyright of Proprietary Materials

INTRAC is a knowledge based organisation. As such Intellectual Property (IP) is a key company asset. Measures to protect this asset are covered in section 4.3. This section is concerned with measures in place to prevent the inadvertent or deliberate misuse of the IP of third parties. INTRAC will respect the IP rights of third parties. This will be done by:

- Acknowledgement, eg where using materials made available through collective commons
- Co-branding of materials as required under contractual arrangements
- Returning background IP as required under contractual arrangements
- Ensuring permission is formally obtained where collective commons or existing contractual provisions are not in place.

Copyright infringement is a serious offense. Reproduction of any copyrighted material without written permission of the owner is a violation of copyright laws, and will not be tolerated at INTRAC. Downloading or uploading of software may be in violation of the copyright, and individuals should review the license agreements to determine the extent of rights associated with software copying, use, and/or distribution. This policy applies to third party software owned or leased by INTRAC, and all proprietary software developed by INTRAC, or works contracted for or purchased/leased by INTRAC.

4.5.1 THREATS/ISSUES ADDRESSED

Making, distributing or using illegal copies of software is in violation of copyright laws. Depending on the nature and extent of the violation, INTRAC and/or its employees could be charged. If found guilty, the Company could be subject to fines, and individuals could receive active jail sentences.

4.6 Availability

Information will be readily available for authorized use when it is needed by the user in the normal performance of his/her duties.

Organisational data must be stored in locations that are subject to regular back up and appropriate access controls. As an example: information relating to contracts with clients should be stored in a location that allows it to be accessed by the job manager, the Business Support team and the Finance Team. The appropriate location of data is detailed in in INTRAC's Data Resource Register.

Whilst it may be temporarily necessary to store some data in other locations (eg use of c:\ or portable storage media whilst working off-line in remote locations) data must be transferred to an appropriate server/cloud location when back on-line.

Arrangements with outsourced IT services will include off-site back-up and recovery for server data.

Appropriate processes will be developed and implemented to ensure the reasonable and timely recovery of all company information, regardless of platform, should that information become corrupted, destroyed, or unavailable for an extended period. For some systems (eg the finance system) this will mean regular use of internal back-up systems as well as server back-ups.

Business impact analysis will be performed periodically to determine the most critical information assets, and establish a schedule for backup and recovery for those most critical systems to ensure their timely recovery in the event of an extended outage.

4.6.1 THREATS/ISSUES ADDRESSED

The unavailability or destruction of corporate information could seriously impact the Company's ability to conduct normal business operations, or cause a significant loss of revenue. Loss of critical information could:

- cause harm to INTRAC's customers,
- be in violation of certain regulatory agencies rules and regulations if certain data is not readily available (eg Tax).

5 ROLES AND RESPONSIBILITIES

5.1 Management

Management must educate their employees with regard to information security issues. Managers will explain the issues, why the policy has been established, and what role(s) the employees have in safeguarding information assets. Consequences of non-compliance should also be explained.

5.2 Employees

Information security is the responsibility of every employee. Employees must adhere to all security policies, procedures and standards. Security guidelines should be followed whenever possible. Any breaches of security, or suspected breaches, should be reported immediately to their management and the Office Admin Manager and our outsourced IT support.

5.3 Contractors, Vendors, other non-employees

All other individuals working at INTRAC are subject to the same information security policies, procedures, and standards as employees. Violation of these rules can result in termination of the contract and/or prosecution, depending on the nature and severity of the event.

5.4 INTRAC Office Admin Manager, Finance and Admin Director and Outsourced IT Support

The INTRAC Finance and Admin Director has the primary responsibility for managing all of the INTRAC information security processes. The following are some of their major functions:

- Ensure adequate outsourced IT support to develop, implement and maintain the corporate information security architecture,
- Determine the need for and develop/modify information security policies and standards to address new or expanded exposures to INTRAC computing resources, in consultation with outsourced IT support,

The INTRAC Office Admin Manager will act as the primary point of contact between INTRAC and its outsourced IT support function. The following are their major functions

- Act as first point of contract for notification of any suspected/potential breaches of security including, loss of equipment and loss of data
- Co-ordinating fact-finding and liaison with outsourced IT function

- Alerting the Finance and Admin Director and the Executive Director where appropriate, and in particular where personal data and contractual relationships are involved. See INTRAC's Data Protection Policy for more details

The role of INTRAC's outsourced IT function is to

- Advice on appropriate security measures
- Implement agreed solutions
- Investigate relevant security breaches or suspected breaches in a timely manner, and report the results to the Finance and Admin Director.

5.5 Senior Management Team

The Senior Management Team shall, at a minimum

- Develop and review information security and business continuity policies,
- Ensure the coordination of the implementation of security strategies, architectures, policies and standards across the INTRAC,
- Review the assessments of security techniques and processes to ensure a good balance of business need, risk and security is achieved.

5.6 Board

The Board of INTRAC shall, at a minimum:

- review and approve information security and business continuity policies,

6 COMPLIANCE

Compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues, and protecting INTRAC's information assets.

Any non-compliance with this or policy that results in the compromise of INTRAC information confidentiality, integrity and/or availability may result in disciplinary action up to and including summary dismissal from the Company, and possible prosecution under applicable laws.

7 ENFORCEMENT AND VIOLATION HANDLING

Any compromise or suspected compromise of this policy must be reported to the appropriate management, and INTRAC Finance and Admin Director, of, if the Finance and Admin Director is involved, to the Chief Executive.