IT Information Security Policy

GOAL IT Security policy

Member:	• all board members/trustees, board committee members and company members of each of GOAL, GOAL (International) and GOAL USA Fund, together with GOAL's branches/liaison offices in programme countries. • all GOAL employees (Head Office and Field), secondees, interns and volunteers; and • all consultants/contractors/suppliers* (including internal consultants with a GOAL email address) • all GOAL partners* * must adhere to either: GOAL's IT Information Security Policy, in which case they shall implement their own reporting and management system; or their own internal, corresponding policy with standards equivalent to GOAL's Acceptable Use Policy. In either case, they shall certify compliance to GOAL periodically.
Title:	IT Information Security Policy
Document type:	Policy
Date/version:	04/02/2019
Classification:	General Distribution
Authors:	Louise Kelly
Owned by:	IT and Human Resources
Reviewed and approved by:	Audit and Risk Advisory Board: 12/08/2019 GOAL Board of Directors: 12/08/2019
Next review date:	March 2021
Related Policy, Procedures, Guidance and Manuals	GOAL IT Acceptable Use Policy GOAL Personal Device Standards and Guidelines GOAL Data Governance and Classification Guidelines GOAL Data Protection Policy GOAL Retention and destruction Guidelines GOAL Social Media & OM Policy GOAL Email Guidelines GOAL Password management Guidelines GOAL's Employee Handbook/Manual (as applicable) GOAL's Whistleblowing Policy GOAL's Data Breach Process GOAL's IT Security Incident Management Process GOALs patch management guidelines GOALs application security and development guidelines GOAL IT Hardware Minimum Specifications

Table of Contents

1 Introduction 4
1.1 Scope 5
1.2 Purpose 5
1.3 IT Security Governance 5
1.4 Oversight 5
1.5 Roles and Responsibilities 6
2 Policy Text 6
2.1 Confidentiality 6
2.1.1 Data Classification and Management 6
2.1.2 Network Security 7
2.1.3 User Authentication and Audit Logging 7
2.1.4 Encryption & Data protection 7
2.1.5 IT Security training 8
2.2 Integrity 8
2.2.1 User Access and Audit Logging 8
2.2.2 Vulnerability Management 9
2.2.3 Change Management 9
2.3 Availability 9
2.3.1 Disaster Recovery and Backup Strategy 9
2.3.2 Incident Management 10
2.3.3 Security Operations 10
2.3.4 Physical computer storage Environmental provisions 10
3 Raising Concern 10
4 Communication and Training 10
5 Compliance with this Policy 10
6 National Laws 11
7 Data Protection 11

1. Introduction

GOAL Information Technology (IT) Security Policy is managed through the below Framework which comprises: (i) this Policy, (ii) Standards and (iii) Procedures, alongside supporting Governance processes. This Framework provides a flexible and effective platform upon which the Policy objectives are met.

The Framework is detailed below:

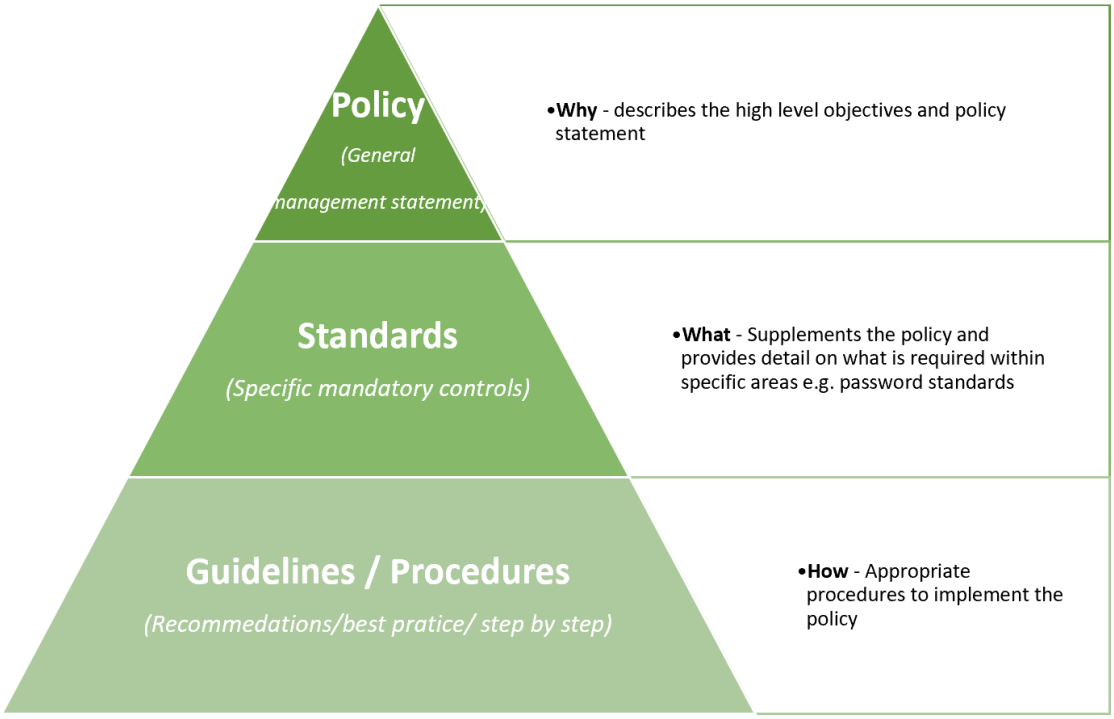

Figure 1

This Policy can be met by adopting and complying with the associated Standards/Guidelines. However, the Framework is designed to be flexible and allow a range of methods to meet this Policy. It enables local autonomy in how the outcomes and objectives of this Policy are met, by allowing local procedural methods and/or controls to be implemented. At the same time, it allows those who require further advice from the IT Department to meet this Policy through the methods detailed in the Procedures. Regardless of the approach, all within scope of the Policy are required to meet this Policy and the Standards using appropriate methods.

It is important to note that the Standards, as outlined in the associated documentation, must be considered the minimum requirements. Where additional information security controls are required for legal, regulatory or governance purposes, the controls must be enhanced accordingly. The IT department can provide advice on how to comply with additional requirements, where required.

This Policy takes precedence over any policies which may be developed at a Country Office level.

1.1 Scope

This IT Information Security Policy covers documentation of policy, procedures and standards relating to:

- GOAL Information Assets
- GOAL IT Resources

This Policy applies to all Users of the GOAL's IT resources which includes, without limitation, its networks (accessed on site or remotely) and/or communications devices.

1.2 Purpose

The purpose of this IT Information Security Policy is to protect the information assets entrusted to GOAL from all threats, internal, external, deliberate or accidental. The policy is aimed at:

- Safeguarding the availability, confidentiality and integrity of Data entrusted to GOAL.
- Protecting the IT assets and services of GOAL against unauthorised access, intrusion, disruption or other damage.
- Ensuring compliance with applicable legislation and regulations.
- Providing a governance structure with clear lines of responsibility and accountability.

The policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents.

1.3 IT Security Governance

IT Security governance is overseen by the CEO, Chief Technology & Business development Officer, with reporting to the Audit and Risk committee at board level.

Policies, procedures and controls are reviewed during the year via a number of mechanisms:

- **Internal Audit**: Security and policy reviews are included in Internal audits, and recommendations to improve the control systems and their implementation is monitored via the Consolidated Issues List. Consolidated information is reported up to the Audit and Risk committee.
- **Risk Register:** IT is a category on the global risk register, with Country programmes and HQ department scoring the risk and mitigation plans. Consolidated information is reported up to the Audit and Risk committee.
- **External Audit:** Statutory external audit scope of work includes a review of financial systems and controls

1.4 Oversight

Compliance with this IT Information Security Policy for each of Head Office, Field Offices and Board/Committee/Member is controlled and monitored on a scheduled basis by the Technology Advisory Board. High level information is reported to the Technology Advisory Board on a quarterly basis.

1.1.1. The Chief Technology Officer reports on technology matters to the Technology Advisory Board on a scheduled basis.

1.1.2. Regional Directors and Country Directors can review and monitor compliance with this IT Security Policy for their respective countries of operations only, raising or reporting any issues that may arise, and to analyse any trends to enhance awareness within the organisation and further learning and development in this area. Global trends will be reviewed and monitored by the Chief Technology Officer.

1.5 Roles and Responsibilities

All users and staff are required to demonstrate compliance to GOAL's IT Information Security Policy in order to protect the confidentiality, integrity, and availability of GOAL's Information Assets. This policy also extends to contractors, consultants and/or 3rd parties providing services to GOAL.

- GOALs IT Department both at Head Office and in country are responsible for monitoring the use of GOAL IT Resources to ensure this Policy is not breached.
- The IT Department/Security Officer is responsible for enforcing effective operation of the GOAL's IT Information Security Policy to ensure that information assets and technologies are adequately protected.
- GOAL Senior Management and Country Management are responsible for ensuring policies and procedures are adhered to throughout their areas of responsibilities.
- GOAL Board are responsible for the oversight, governance and support of GOAL's IT Information Security Policy.

2 Policy Text

2.1 Confidentiality

Safeguarding the confidentiality of information through the protection of information from unauthorised disclosure with access only by entitlement.

2.1.1 Data Classification and Management

- GOAL is obligated to respect the rights of individuals and to protect confidential data.
- GOAL's Data Protection Policy should always be adhered to
- All digital records should be classified according to the GOAL Data Governance and Classification Guidelines.
- When data is classified as confidential data, appropriate access and security controls are applied in transmission and storage. Confidential data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data. Please refer to Data Management Guidelines.
- All GOAL information is to be treated as confidential if not otherwise indicated.
- Where GOAL engages the use of Cloud or external hosting services, which will host data, terms and conditions but be reviewed and the proposed solutions must be evaluated by the GOAL IT Department per the following GOAL's Third Party Hosting Information Security Questionnaire.
- Where data and servers on a GOAL network are accessed by 3rd parties (suppliers, contractors, consultants) for support and maintenance provided to GOAL, Third Party Access forms with the accompanying Data Protection and Non-Disclosure agreements (where applicable) must be built into the service agreement with the Third Party.

2.1.2 Network Security

- GOAL maintains a perimeter firewall on our networks. All externally facing services must be registered, this register is used to configure the firewall based on the services they offer. This reduces targeted cyber-attacks from the internet while allowing access to registered services.
- In addition to the perimeter firewall, some network ranges are protected by access-lists or additional firewalls.
- Perimeter traffic is logged and appropriately monitored for security purposes.
- Laptops and Desktops that connect to a GOAL network should have:
  - Anti-virus installed and up-to-date,
  - Operating System patched with latest security updates
  - Personal Firewall active
  - User authentication
  - Encryption
  - Genuine licenced software as per GOAL Approved Software list.

2.1.3 User Authentication and Audit Logging

- Authentication is required for each connection to the network.
- Where possible Two factor authentication should be considered for IT Systems that process sensitive data.
- All IT systems must comply to GOAL's Password Management Guidelines.
- User must follow best practices to prevent misuse, loss or unauthorised access to systems:
  - Keep passwords confidential
  - Change passwords regularly
  - Never write down passwords
  - Never send passwords via email, fax or post
  - Change temporary passwords at first logon
- Do not leave your computer unattended without locking your computer or logging off.
- Audit logs containing the following user events of staff, and any 3rd parties accessing GOALs network are captured and monitored:
  - User IDs
  - Dates and times for logon and logoff
  - Device identity and location where possible
  - Records of successful and rejected system access attempts
  - Monitoring of privileged user accounts

2.1.4 Encryption & Data protection

- All GOAL owned laptops must have their internal hard drive encrypted. This is a service supported by GOALs IT Department per Encryption Guidelines
- All GOAL provided mobile devices that host data (email, OneDrive, SharePoint) must be protected by encryption and layered authentication where appropriate.

- Where personal or sensitive data is being stored on a laptop or portable device, mobiles phones etc, GOAL owned or personal, then this device/data should be encrypted in accordance with the encryption guidelines and ensure compliance with the GOAL Data Protection policy
- Where sensitive information is transmitted through a public network to an external third party the information must be encrypted first and sent via secure channels (SFTP, SSL, HTTPS, VPN etc.)
- WI-FI networks managed for staff business, must be encrypted using WPA2 or better.
- Guest Wi-Fi network must be applied at each network if possible

2.1.5 IT Security training

- IT Security awareness strategy is delivered through multiple methods with the aim of raising user awareness and highlighting end user responsibilities.
- Scheduled, targeted and on-demand Security Awareness Training sessions are available in conjunction with Data Protection training.
- On staff induction new hires are briefed on, receive a copy and sign the Data Protection Policy and the IT Acceptable Use Policy.

2.2 Integrity

Safeguarding the integrity of information, i.e. the accuracy and completeness of information by protecting against unauthorised modification.

2.2.1 User Access and Audit Logging

- Access to information is granted on a need only basis, staff are granted specific access to allow them to carry out their job functions. This would be done in accordance with the principle of least privileges.
- Access to amend information and/or access to systems which process and record this information is restricted to authorised personnel.
- All individuals have a unique user ID (end users, DBA's, network admin, programmers) for their personal and sole use so that activities can be traced to the responsible person
- Access to code, OS, services and commands is restricted to only those individuals who require access as part of their day-to-day job responsibilities.
- All access to high criticality services are logged and appropriately monitored to identify potential misuse of systems or information. Logs are retained, and access granted according to the appropriate legislation.
- Security event logs, operational audit logs, error logs, transaction and processing logs are monitored on critical systems and retained to record events for trouble shooting, provide forensics during security incidents and to identify potential misuse of systems or information.
- An appropriate audit trail including database logs of the creation, amendment and deletion of GOAL data and/or systems is maintained by GOALs IT Department. This is particularly important in relation to the following:
    - Data including details on staff, beneficiaries and suppliers;
    - Data including inward fee payments, outward supplier payments, and payroll transactions;
    - GOAL resource usage data.

- GOAL data which may reside outside main GOAL system(s). This could include data which resides on external cloud services or data that resides on internal such as Excel Spreadsheets, local desktop databases etc.

2.2.2 Vulnerability Management

IT staff are responsible for ensuring that the equipment connecting to a GOAL network is configured correctly, that the operating systems and software applications are up-to-date in accordance to GOALs patch management guidelines and that the equipment has adequate protection against viruses and other malware. If there is any suspicion that the equipment may be infected or compromised, it should not be connected.

- GOAL infrastructure (servers, desktops, operating systems, databases and applications) must follow a regular patch schedule to ensure IT Assets remain protected from security vulnerabilities and remain within mainstream support.
- Antivirus is compulsory pre-requisite for any computer joining the GOAL network. Anti-virus is controlled centrally from GOALs IT Department.
- The GOAL's IT Department has the authority to remove from the network any equipment for which no owner can be identified.
- The GOAL's IT Department has the authority to remove from the network any equipment which is interfering with the network service or is deemed likely to compromise the security of the network. While every effort will be made to contact the owner of the equipment in advance, maintaining the service must take precedence.

2.2.3 Change Management

System changes and development should be completed in accordance with the IT Department formal change management process through the Business Change Management tool with audit trails for changes to highly critical systems and in accordance to GOALs application security and development guidelines

2.3 Availability

Maintaining the availability of the GOAL's information and IT systems for business processes usage as required.

- Each IT Service has a defined service owner. The service owner must ensure that all software licenses are up-to-date, and that maintenance support is available for both the hardware and software associated with their service.
- Desktop software licencing for standard software is managed centrally through site licensing for staff. Licensing for non-standard software is the user's responsibility.
- Illegal and unlicensed software must not be installed on GOAL owned computers. IT Equipment must be procured and configured to GOALs minimum specifications

2.3.1 Disaster Recovery and Backup Strategy

- It is the responsibility of the business owner of each service to ensure that an adequate business continuity plan is in place in the event that the service is affected by the non-availability of the relevant servers, network or other elements of the IT infrastructure, including the prevention of data loss through data back-ups.

- GOALs IT Department maintain Disaster Recovery plans for all GOAL centrally managed infrastructure and critical services.
- Disaster Recovery plans and processes are tested regularly.
- GOALs IT Department manage Data and system backups for critical systems
- Recovery from backup is tested regularly

2.3.2 Incident Management

Formal incident management procedures are in place for IT Security incidents and procedures relating to personal data breaches. Please reference GOALs IT Security Incident Management Process and GOALs Data Breach process.

Lost or stolen devices must be reported to the Logistics and IT department within 24 hours. Followed by filling the damage lost report.

2.3.3 Security Operations

GOALs IT Department manage multiple security tools with the aim of protecting the IT assets and services of the GOAL against unauthorised access, intrusion and disruption. Processes are in place to support these tools and ensure proactive management of IT vulnerabilities and reported incidents.

2.3.4 Physical computer storage Environmental provisions

Any servers hosting production services for the GOAL must be housed where possible in a suitable environment with regard to security, electrical power, air cooling etc.

- All hardware used for the storage of GOAL data is to be purged of data and securely destroyed once it is no longer to be used. See GOAL Retention and destruction guidelines.
- When tapes and other secondary storage devices reach the end of their useful life, they are to be purged of GOAL Data and securely destroyed.

3 Raising Concern

If you have a concern with regard to other GOAL Members' compliance with this IT Security Policy, please consult our Whistleblowing Policy on SharePoint or email speakup@goal.ie in confidence. In addition, if you have a serious concern over a wrongdoing, please contact goal@safecall.co.uk or call 1800 812740. Please note each country may have a different Safecall number.

4 Communication and Training

4.1. GOAL will effectively communicate and provide training on this IT Security Policy to all Members on induction/appointment.

4.2. This IT Security Policy will be reviewed annually.

5 Compliance with this Policy

5.1. Any violations of this IT Security Policy will be dealt with in accordance with GOAL's Disciplinary Procedure and may result in a disciplinary sanction up to and including termination of employment or removal from a GOAL board, or expulsion from being a committee member or company member.

5.2. GOAL reserves the right to report any suspected fraudulent or criminal activities to the relevant authorities.

6 National Laws

For the avoidance of doubt, this IT Security Policy supplements national laws and related fiduciary duties, including but not limited to applicable company and charity law.

7 Data Protection

Any information provided to GOAL under this IT Security Policy will be processed in accordance with applicable data protection law and for the purposes set out herein. This will include the processing of information to ensure that Members act in the best interests of GOAL and that GOAL complies with the requirements of all donor contracts. Such information will be also declared in GOAL's accounts and annual report where required under applicable law or accounting guidelines.