INFORMATION SECURITY POLICY

Document Reference:	EN_GPSecPol-01
Version:	1.1
Date:	28/02/2022
Domain:	Information Security
Classification:	Public

THE HUMAN
EXPERIENCE
COMPANY

SUMMARY

01

PREAMBLE

1 Preamble

1.1 INTRODUCTION

In the current digital era, information security risks are becoming more and more prevalent across the globe, impacting business strategies, visions and objectives, and in extreme cases an organisation's survivability. Webhelp takes information security very seriously and takes the treating of risk as a priority.

At Webhelp we acknowledge and understand our responsibilities to ensure the safe guardianship of any information entrusted to us whether client, supplier, or other stakeholder's. Failing to protect such information could potentially harm individuals' rights, negatively impact our clients and/or Webhelp's reputation and brand, whilst also potentially leading to regulatory sanctions and financial penalties or other forms of liabilities and losses.

The Webhelp Global Information Security Policy has been developed to ensure a robust, effective, and continuously improving Information Security Management System (ISMS) and is maintained globally by all business units, all regions, and all entities that comprise Webhelp and its related businesses. For the purpose of this document, Webhelp shall mean (i) Webhelp SAS (ii) all Affiliates (iii) wholly owned subsidiaries of Webhelp SAS.

1.2 INFORMATION SECURITY OBJECTIVES

Our Vision

"To embed security and support business growth and efficiency through a service-oriented model, providing a pragmatic, risk-based approach to managing information security risks."

The Webhelp Global Information Security Policy sets the foundations for achieving our vision by maintaining a globally consistent approach in:

- Achieving business objectives *securely*.
- Retaining the trust of our people, clients, suppliers, and other stakeholders.
- Protecting informational assets against potential or actual, emerging or projected, internal or external and deliberate or accidental threats.
- Maintaining information confidentiality consistently and in accordance with its level of classification.
- Ensuring information integrity.
- Ensuring the availability of information when needed.
- Meeting regulatory, statutory, and contractual requirements.
- Respecting data subject rights.
- Protecting our clients and the Webhelp brand.

This is performed through our implementation of an Information Security Management System (ISMS) that follows globally accepted best practices and incorporates various global standards, best practices, and regulations, e.g., ISO27001:2013 (and the relevant code of practice ISO27002:2013), PCI DSS, NIST CSF, SOC2, the GDPR, HIPAA and other relevant Data Privacy laws. This way, we ensure that:

- Information security policies, standards and procedures are established, maintained and communicated.
- Top level management plays an integral part in setting Specific, Measurable, Achievable, Relevant and Timely (SMART) objectives that are reviewed and audited against at planned intervals.
- Accountability for information security is assigned to dedicated resources with the requisite expertise at appropriate Webhelp levels (global, entity, etc.).
- Information security risks are identified and treated in accordance with their criticality level to remain within risk appetite.
- Information security training is available and mandatory for all employees.
- Information security controls are implemented, and their effectiveness continuously measured and improved.
- Information security incidents are identified and managed in a timely manner.
- Compliance with regulatory, statutory, contractual, and internal policy obligations is monitored and achieved.

1.3 ISMS SCOPE

The Scope includes all Webhelp's operational procedures in relation to determining, administering, and maintaining outsourced customer services and customer insights and data analytics services.
This is inclusive of:

- Client information held by Webhelp.
- Systems held or operated by Webhelp on behalf of clients to deliver services.
- Information that is the intellectual property of Webhelp.
- Personal information relating to employees of Webhelp.
- Sites & equipment managed by Webhelp.
- Personnel, IT systems, manual systems, tools, utilities, and data participating or managed in Webhelp day-to-day operations.

02

ISMS POLICY STATEMENTS

2 ISMS Policy Statements

2.1 PERSONNEL RESPONSIBILITIES

All Webhelp personnel, contractors and 3rd parties with access to corporate premises, information systems and data must conduct themselves in accordance with Webhelp's principles, values, Code of Conduct, and information security policies.

Personnel responsibilities and competencies on information security must be assigned, communicated, and agreed on prior to employment, and stay in effect during and after termination of employment or contract. In addition, all Webhelp employees and relevant 3rd parties must agree and comply with Webhelp's Acceptable Use Policy. Conformance with those responsibilities must be reviewed and verified on a constant basis.

Regular security and privacy awareness training must be provided, including simulations of plausible information security incident scenarios, newsletters, and other communication methods, to ensure all personnel stay current on their responsibilities against information security risks.

2.2 DATA PROTECTION

Data collected, generated, stored, maintained, and disposed of by Webhelp or on behalf of Webhelp, must always be identified and protected against information security risks according to its sensitivity and classification.

Data management procedures must be established and implemented to ensure the confidentiality, integrity, and availability of information during its whole lifecycle, to achieve secure, uninterrupted operations and agreed service levels.

Data must be handled according to its sensitivity from collection to disposal, in accordance with global, regional, and country legal, statutory, and contractual requirements. Adherence to the requirements must be measured on a constant basis.

2.3 OPERATIONAL SECURITY

Critical information systems operated by or on behalf of Webhelp must always be protected against information security risks. Malicious or accidental compromises must be detected and responded to in a timely manner.

A defence-in-depth approach must be followed by implementing several layers of information security controls, to enable the prevention of information security incidents. Controls must cover physical security mechanisms, network layer protection mechanisms, endpoint secure configuration baselines, secure application development procedures, and least-privilege access controls.

To minimise the impact of a potential preventive information security control failure, detective information security controls coupled with a 24/7 monitoring and response capability must also be implemented. This should enable the early detection of threats to the confidentiality, integrity, and availability of information and information systems, timely escalation, response, and resolution.

2.4 SUPPLIER SECURITY

All suppliers that store or access Webhelp (or Webhelp clients') data must abide by applicable laws and the information security requirements set out in signed agreements.

Prior to contracting with suppliers who may access Webhelp information, a robust due diligence process must be followed and requirements for addressing information security risks relevant to such access must be agreed. This process must follow Webhelp's principles and policies and client's potential specific requirements and flow-downs.

Adherence to the information security requirements set out in supplier agreements must be monitored and evaluated at planned intervals. Failure by a supplier to comply with its contractual obligations relating to information security must be treated as a material breach immediately remedied to safeguard the affected data. All applicable remedies (including injunctive relief, financial liability and/or termination of the agreement) must be considered. Discrepancies must be reported and treated in a timely manner following a risk-based approach.

2.5 RESILIENCE

Business-critical resources, including people, information, and information systems, must remain operable or be recoverable at an operable state after a defined timeframe, in the event of an information security incident or other unplanned event.

Business continuity and disaster recovery strategies must be established and implemented to allow business critical service continuity in a timely manner after an unplanned event occurs. Special attention to be given on recovering information security controls so that recovered services are performed securely.

To ensure business continuity and disaster recovery strategies can be executed as intended when an unplanned event occurs, proactive testing must be performed at planned intervals. Testing should include, amongst others, simulating plausible information security incident scenarios (e.g., ransomware).

2.6 RISK MANAGEMENT

Information security risks must be regularly assessed, their likelihood of being realised and their potential impact rated and if not within risk appetite, treated.

Changes to the threat landscape that may result in new or increased information security risks must constantly be assessed through a continuous risk management programme. Information security risks must be considered as part of the broader enterprise risks, allowing Webhelp senior management a holistic view of risks enabling their informed decisions on required treatment.

A Risk Management Framework must be established and maintained, that defines an end-to-end approach from risk identification, analysis, and documentation in risk registers, to mapping against existing controls, tracking risk mitigation activities, and reporting the results of such activities on a regular basis. The Framework must guarantee a balance between the level of risk, the controls selected for its mitigation and the nature of the information.

2.7 COMPLIANCE

Compliance with global, regional, and country laws and regulations, contractual requirements, information security standards, voluntary certifications and internal policies must always be upheld.

An effective compliance programme evaluating information security and data privacy controls must be established and maintained at planned intervals. The programme must be transparent on the overall sufficiency and effectiveness of the information security and data privacy environment.

Adherence of the ISMS to information security standards (e.g., PCI-DSS) and voluntary certifications (e.g., ISO27001) must be reviewed by Webhelp senior management and audited by independent practitioners as defined by each standard. Evidence of adherence should be made available to interested parties upon request.

2.8 CONTINUAL IMPROVEMENT

The ISMS must be constantly evaluated and improved to better address existing, emerging, and projected information security threats and risks.

A quality assurance programme must be established and maintained to ensure and improve the suitability, adequacy, and effectiveness of the ISMS against the ever-changing information security threat landscape.

Proactive measures must be taken to identify and assess changes in information security risks. Where the ISMS is deemed ineffective on addressing those risks, corrective actions must be planned, implemented, and communicated in a timely manner.

03

DOCUMENT CONTROL

3 Document Control

VERSION	DATE	SUMMARY	OWNER
0.1	08/03/2021	New Draft Policy for internal review	Webhelp Global Security (WGS)
0.2	10/03/2021	Changes/additions by WH Legal team	WGS
1.0	15/03/2021	Final Release	WGS
1.1	24/01/2022	Annual Review. The following minor changes were made: 1. Typos amended 2. Added standards/regulations this policy must comply with after Webhelp acquisition of OneLink 3. Added Risk Management section to add clarity as this was previously considered embedded	WGS
1.1	28/02/2022	Approved by WH Group Information Security Steering Committee (GISSC)	GISSC

Review Frequency	This policy will be reviewed at least annually or upon significant business change
More Information	Webhelp Global Security (WGS)
Date of Issue	28/02/2022

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to infosec@webhelp.com or your line manager.