The Bridge Group Ltd
http://www.thetrustbridge.co/

Anti Slavery- Human Trafficking- Human Rights Policy

Security Incident Reporting Quick Reference

Note! Regardless of confidence level, all security incidents must be immediately reported by email and phone So even if the security incident is only potential or suspected—it must still be reported without delay.

Contact by Mail and Phone	Comment
david@thetrustbridge.co	Use email and phone below
2071752476	2071752476
"The Firm"/The Bridge Group Ltd	The Bridge Group Ltd

Document Approval

This document has been approved by the following

Role	Name	Version Details
CEO The Bridge Group Ltd	Penny Heyes	See section 14.4 Version Control, and section 14 Document Control

Contents

1. Overview

Modern slavery is a crime and a violation of fundamental human rights. It takes various forms, such as slavery, servitude, forced and compulsory labour and human trafficking, all of which have in common the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain.

2. Policy Statement

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, agents, contractors and suppliers.

3. Suppliers Expectation

The Bridge Group Ltd strictly prohibits the use of modern slavery and human trafficking in our operations and supply chain. The Bridge Group Ltd have and will continue to be committed to implementing systems and controls aimed at ensuring that modern slavery is not taking place anywhere within our organisation or in any of our supply chains. The Bridge Group Ltd expect that all our suppliers will hold their suppliers to these standards.

4. Responsibility for The Policy

The Board of Directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy. Managers will remain alert to indicators of modern slavery and respond appropriately if they find or are informed of any indication of modern slavery.

5. Compliance with Policy

You are encouraged to raise concerns about any issue or suspicion of modern slavery in any parts of our business or supply chains of any supplier tier as soon as possible. There is no typical victim and some victims do not understand they have been exploited and are entitled to help and support. However, the following key signs could indicate that someone may be a slavery or trafficking victim. This list is not exhaustive:

- the person is not in possession of their own passport, identification, travel documents or bank account;
- the person is acting as though they are being instructed or coached by someone else;

- they allow others to speak for them when spoken to directly;
- they are dropped off and collected from work;
- the person is withdrawn or they appear frightened;
- the person does not seem to be able to contact friends or family freely; and
- the person has limited social interaction or contact with people outside their immediate environment.

6. Risk Assessments

The Bridge Group Ltd take a risk based approach to our contracting processes and keep them under regular review.

The Bridge Group Ltd assess whether the circumstances warrant the inclusion of specific prohibitions against the use of modern slavery and trafficked labour in our contracts with third parties.

Using The Bridge Group Ltd's risked based approach we will also assess the merits of writing to suppliers requiring them to comply with our Code of Conduct, which sets out the standards required to combat modern slavery and trafficking.

Consistent with The Bridge Group Ltd's risk based approach we may require:

employment and recruitment agencies and other third parties supplying workers to our organisation to verify their compliance with our Code of Conduct

Suppliers engaging workers through a third party to obtain that third parties' agreement to follow the Code

As part of The Bridge Group Ltd's ongoing risk assessment and due diligence processes we may consider whether circumstances require us to carry out audits of suppliers for their compliance with our Code of Conduct.

If The Bridge Group Ltd discover that individuals or organisations working on our behalf have breached this policy, we will ensure that appropriate action is taken. This may include by the breach to terminating the relationship

7. Breaches of policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to The Bridge Group Ltd's assets, or an event which is in breach of The Bridge Group Ltd's security procedures and policies.

All The Bridge Group Ltd's employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through The Bridge Group Ltd's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of The Bridge Group Ltd.

The Bridge Group Ltd will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

For more information, see Security Incident Management Policy.

All users of The Bridge Group Ltd's ICT facilities must comply with this policy and be aware of the Policy.

This document forms part of The Bridge Group Ltd's Policy and as such, must be fully complied with.

8. Scope

The scope of this policy extends to all departments, employees, contractors, vendors and partner agencies who use/access The Bridge Group Ltd's ICT facilities.

9. Purpose

The purpose of this Acceptable Policy is to apply acceptable use controls to Information, Information Systems, software Applications, Communication Networks, and mobile devices, used throughout.

10. Definitions

Term	Description
Information	Any information, data or record irrespective of format, collected, generated or used by a business system or process. Examples include electronic communications, emails, digital recordings such as Call Centre Telephone conversations and CCTV, hard copy (paper) files, photographs, maps, plans, process documentation (code, scripts, etc.) and technical drawings.
Information Classification	Assigning a piece of information to a particular category based on its content
Information [Asset] Owners	Executive and Senior managers who are responsible for managing the acquisition, creation, maintenance, usage and disposal of The Bridge Group Ltd's Information and Information Systems within their assigned area of control
Information Risk	That part of The Bridge Group Ltd's overall risk portfolio which relate to the confidentiality, integrity and availability of information within The Bridge Group Ltd.
Information Security	The ability to protect the confidentiality, integrity and availability of information held by The Bridge Group Ltd, including any sub-contractors and suppliers, from unauthorised use, disclosure, modification, damage or destruction be it accidental or malicious.
Information Security Breach	An Information Security Incident where it is confirmed that a stated organisation policy or legal requirement regarding Information Security has been contravened.
Information Security Incident	Any event/information that warrants concern by Business Information Security that may also possibly affect Business Customer information systems, clients, or business partners.
Information System	Information in any media type, hardware, software, supporting networks, processes and human resources that support its acquisition, processing, storage and communication.
Secure	A term used in this document to define the requirement to manage information in a manner so as to minimise the risk of a Security Incident occurring through unauthorised disclosure or access to classified information
The Business	The Bridge Group Ltd classified as Private Limited Business
The Business Personnel	Includes all The Bridge Group Ltd's employees as well as all temporary staff, contractors, consultants and any third party with whom special arrangements have been made e.g. Confidentiality and Non-Disclosure Agreements.
CTO	Chief Technology Officer
Security Forum	The Bridge Group Ltd's forum where information security matters are discussed and activities related to information security are co-ordinated.
ICT	ICT, or information and communications technology

11. Duties and Responsibilities for Information Security

Role or Team	Description
Chief Executive Officer	Has overall accountability and responsibility for Information Security within The Bridge Group Ltd on a day-to-day basis the Information Security Lead will be the CEO as the Senior Information Risk Owner.
Senior Information Risk Owner (SIRO)/ CEO	Will act as the advocate for information risk on the Business Board and in internal discussions, and will provide written advice to the Chief Executive Officer on the content of their annual statement in regard to Information Risk.
Human Resources	Shall be responsible for ensuring that suitable contracts and non-disclosure agreements are in place with external contractors before access to The Bridge Group Ltd's Information is given. These contracts require the contractor to comply with all appropriate security policies.
IT Systems and Data Manager	Is responsible for the implementation and enforcement of the Information Security Policy.
Line Managers	Are responsible for ensuring that all their staff (permanent and temporary) and contractors are aware of the Information Security Policy and that it is implemented fully in their area of responsibility.
Procurement	Shall be responsible for ensuring that suitable contracts with non-disclosure clauses are in place before access to The Bridge Group Ltd's Information is given. These contracts shall ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.
Security Forum	Is responsible for ensuring that The Bridge Group Ltd complies with the Data Protection Legislation and as amended and that Information Governance standards are effectively managed and implemented.

12. Policy Review

This policy will provide a measure against which information security incidents can be assessed and subsequently managed.

The Bridge Group Ltd (via the Security Forum) will review this policy on an annual basis or in response to an actual or perceived increase in information security risk.

13. References

These references below are those most directly relevant.

#	Title	Description	Comment
1	500140 Legislation List	Current list of legislation relevant to The Bridge Group Ltd	This is likely to be updated so always check for the latest version

14. Document Control

14.1. Contributors, Reviewers ,and Approvers

#	Role	Name	Comment
1	Approver – The Bridge Group Ltd	Penny Heyes CEO	
2	Content Author		
3	Reviewer	David Clarke	
4	Producer		

14.2. Document Maintenance

This section holds central information, it includes 'bookmarked' data which can then be reflected into other parts of the document.

#	Name	Date	Description	Comment
1	Next Review Date	22/01/2024	The latest date by which this document needs to be reviewed	This document is intended to be reviewed annually by the Security Forum. It can be reviewed prior to date here. This will be set when the document is Released

14.3. Document Access Control Categories

The access categories/classifications in use

#	Category (Classification)	Circulation	Comment
1	Controlled	Can only be circulated to The Bridge Group Ltd personnel, and selected approved business partners/third party suppliers	
2	The Business	The Bridge Group Ltd	The list for Read/write/edit is provisional and can be extended

14.4. Version Control

Version	Status	Actions	Action By	Date Started
0.1	Draft	Initial draft: replaced all previous information security polices		
1.0	Released	Reviewed and Amended for Final Release		
1.1	Released	Minor amendments		22/02/2023

14.5. Applied ISO27001 Controls

Control Ref	Title
A.7.2.3	Disciplinary process