Document ID	POL050
Document Title	Social Engineering Fraud Policy
Author	Jessie Kelly
Version	5
Classification	Controlled

Revision History		
Date	**Version**	**Change**
14/08/2025	2025084	Annual Review, Template Format
08/04/2026	2026045	Annual Review – No Changes

Distribution		
Date	**Version**	**Distribution**
14/08/2025	2025084	All Staff – Compass, Company Website
08/04/2026	2026045	All Staff – Compass, Company Website

Signed			
Date	**Version**	**Name**	**Role**
14/08/2025	2025084	Tina Sexton	Finance Director

Contents

Introduction

Bytes Software Services Limited ("Bytes") is committed to maintaining the highest ethical standards across all areas of its operations. As part of this commitment, Bytes has established a robust framework to prevent and detect Social Engineering Fraud—a form of deception in which individuals are manipulated into divulging confidential information or performing unauthorised actions, such as making payments or granting access to systems or premises. Social engineering tactics may be employed through various channels, including telephone, email, and face-to-face interactions. This policy outlines the measures in place to safeguard against such threats, supports employees in identifying and responding appropriately to potential risks, and thereby ensures compliance with all relevant UK legislation.

Purpose

Employee behaviour can have a huge impact on information security in organisations and therefore Bytes requires anyone working with the business as an employee or contractor to be constantly cognisant of such fraud.

Scope

This policy requires employees and any person working on behalf of Bytes to act at all times with honesty, integrity, propriety and due care in all matters, but particularly in the safeguarding of Bytes, its associated assets, its reputation and that of its parent.

Policy

Any suspicion of social engineering fraud must be reported to Bytes Finance Director immediately. All reports will be dealt with in a safe and confidential manner (see 'Whistleblowing Policy') and will be investigated rigorously. Any breach of this Policy by a staff member may ultimately lead to dismissal via Bytes disciplinary procedure.

The counter measures implemented by Bytes to prevent, detect and respond to Social Engineering Fraud include but is not limited to:

- Data Classification Assessment
- Verification Procedures
- Additional Verification Checks on all Hardware Orders
- Procedures on all requests for Payment
- No unapproved third-party software / Rogue Devices to be used
- Company Policies in place re Suspicious Unsolicited Emails
- Social Media Outlets constantly monitored
- Only Approved Waste Disposal Carriers used for all waste (hard copies & software)
- Secure physical access to the building & CCTV in operation
- Network password policy in place
- Regular Staff Training & Refresher Training

Responsibilities

Should anyone have a reasonable belief, suspicion or concern that someone has been engaged in social engineering fraud however insignificant it may be and whether it involves an employee or a third party this must be reported to the Finance Director should anyone ever be asked to do something, either by an employee of Bytes or a third- party, where they suspect there may be social engineering fraud, or believe that they are a victim of another form of unlawful activity, this must be reported to the Finance Director.

Should an employee refuse to act on a request, either by an employee of Bytes or a third- party, which they think may result in social engineering fraud and feel worried about the potential consequences, Bytes will support them even if investigation finds that they were mistaken.

Ongoing monitoring

Bytes will maintain an effective system for monitoring compliance procedures to ensure it remains committed to its zero tolerance to social engineering fraud. This includes training and forms part of the induction process for all new employees.

Related Documents

- POL043 - Fraud, Bribery & Money Laundering Policy
- POL039 – Speak Up Policy
- POL018 - Access Policy
- POL014 - User Management Policy