ANTI-FRAUD POLICY

COMPUTER 2000

Revision 01
May 2023

ANTI-FRAUD POLICY

Contents

Introduction

COMPUTER 2000 Bulgaria ("Company") is committed to follow strict legal and ethical requirements.

Fraud and corruption are a persisting threat to businesses. The Company considers this as an extremely important matter and is engaged to the promoting anti-fraud and anti-corruption culture.

This policy provides direction and guidance to those who might be dealing with suspected cases of fraud or corruption.

This document applies to any (suspected) irregularity, involving employees as well as consultants, vendors, contractors, customers and/or any other parties having a business relationship with COMPUTER 2000 Bulgaria.

Definitions

Fraud is any act of deception carried out for the purpose of unfair, undeserved and/or unlawful gain. It may involve manipulation, falsification or alteration of computer or paper data, records or documents; misappropriation (theft) or willful destruction or loss of assets including cash; and deliberate misapplication of accounting or other regulations or policies.

Corruption is the abuse of entrusted power for private gain. It may take many forms, can happen everywhere and involve everyone.

Irregularity is any incident or action which is not part of the normal operation of the system or the expected course of events.

Responsibilities

The Company will undertake investigation where there is suspected fraud and take the appropriate legal and/or disciplinary actions. For proven or suspected cases, the Company will make any necessary changes to systems and procedures to prevent similar occurrences in the future.

Responsible for exercising disciplinary actions is the Company CEO.

Overall accountability for managing the risk of fraud or corruption has been delegated to departments managers. Their responsibilities include:

- ensuring that adequate and up-to-date internal controls and reporting exist within their areas of responsibility;

- preventing and detecting fraud or corruption;
- assessing the types of risk involved in the operations for which they are responsible;
- taking appropriate action to safeguard the recovery of assets.

Fraud detection

Accountable personnel should be alert to the possibility that unusual events or transactions could be symptoms of fraud or attempted fraud. Irregularity may also be brought to management attention by a third party.

The factors which gave rise to the suspicion should be determined and reviewed to clarify whether a genuine mistake has been made or an irregularity has occurred. Preliminary examination may involve discreet enquiries with staff or the review of documents.

Action following detection

When any member of staff suspects that a fraud has occurred, he/she should notify his/her department manager immediately. The initial report can be verbal and must be followed up within 48 hours by a written report addressed to the department manager and Company CEO covering all known details, involved personnel/parties and undertaken actions.

Department manager may undertake an initial inquiry to ascertain the facts. The purpose of the initial enquiry is to confirm or negate, as far as possible, the suspicions that have arisen so that, if necessary, disciplinary action including further and more detailed investigation may be initiated.

Investigation / further action

If it appears that a criminal act has not taken place, an internal investigation will be undertaken to:

- determine the facts;
- consider what, if any, action should be taken against those involved;
- consider what may be done to recover any loss incurred; and
- identify any system weakness and look at how internal controls could be improved to prevent a recurrence.

If the initial examination confirms the suspicion that a fraud has been perpetrated, then to prevent the loss of evidence which may subsequently prove essential for disciplinary action or prosecution, the person heading up the investigation should:

- take steps to ensure that all original evidence is secured as soon as possible;
- be able to account for the security of the evidence at all times after it has initially been secured, including keeping a record of its movement and signatures of all persons to whom the evidence has been transferred. For this purpose, all items of evidence should be individually numbered and descriptively labeled;
- not alter or amend the evidence in any way;
- ensure that electronic evidence is appropriately handled by certified specialists.

Managers conducting initial enquiries must be conscious that internal disciplinary action and/or criminal prosecution may result.

After proper investigation, the Company will take legal and/or disciplinary action in all cases where Company management consider further action appropriate.

Where initial investigations point to the presence of a criminal act, the CEO will contact the police and Company's legal advisers at once. The advice of the police will be followed in taking forward the investigation.

Recovery of losses

The recovery of losses should be a major objective of any fraud investigation. At this point, the quantification of losses is important and is performed by the Company CFO. Repayment of losses should be sought in all cases. Where necessary, the Company will seek external and legal advisors on the most effective actions to secure recovery of losses.

In order to protect the Company from further loss and damage from destruction of evidence, it may be necessary to temporarily suspend the member of staff concerned immediately after the initial report has been made submitted to Company management.

Learning from experience

Following completion of the case, the accountable Department manager should prepare a summary report on the outcome and lessons learned circulating it to all other interested parties who must take the appropriate action to improve controls to mitigate the scope for future recurrence of the fraud. Company management must make any necessary changes to systems and procedures to minimize prospects for similar acts of fraud