WHISTLEBLOWING POLICY

1. GENERAL PROVISIONS

1.1 Scope of the Policy

This Policy describes the internal channel for reporting of Information on Breaches at IBM Romania S.R.L. (the "**Company**", "**we**", "**us**") and the subsequent actions in relation to their processing and has been developed on the grounds of Art. 9, para. 1 of Law no. 361/2022 on the *protection of public interest whistleblowers*[1] *("**Whistleblower Protection Law**")*.

This Policy is an IBM document specific to Romania and concerns the employees, trainees, hire candidates, directors and contractors of IBM Romania S.R.L., as well as any person working under the guidance and supervision of an IBM contractor, regardless of whether they are remunerated or not. This document regulates the procedure for Romania for reporting Breaches at or concerning the Company which fall within the scope of the EU Whistleblowing Directive[2] and the Whistleblower Protection Law. This Policy supplements the "**IBM Group Policy**" which regulates the terms and conditions for submitting concerns via the Employee Concerns program, and which applies for all IBM companies within the IBM group, part of which is IBM Romania S.R.L. In the event of a discrepancy between the IBM Group Policy and this Policy, the procedures set out in this Policy shall apply where the reported Breaches fall within the scope of the Romanian Whistleblower Protection Law and are within the areas listed in section 3 below. This does not necessarily mean that the employees of the Company are restricted from using all available means for reporting a Breach as offered by IBM, as they choose to do. In such cases, any Report which falls under the scope of this Policy shall be transferred to the Contact Persons to be reviewed under this Policy.

The possibility of reporting Breaches is open not only to our employees but for all persons who have received Information about Breaches at or concerning the Company, during or in connection with the performance of their employment or work duties or in any other professional context. The procedure described below applies to all Reports related to Breaches within the scope of the Whistleblower Protection Law.

1.2 Purpose of the Policy

It is essential for a functioning compliance system to recognise and address Breaches at an early stage so they can be remedied without delay and the current system can be adapted, if necessary. This requires that all employees are vigilant and willing to report if they consider that they have Information on actual or potential Breach within the scope of section 3 of this Policy. The Company has therefore implemented an internal reporting channel that provides confidential means of communication to report possible Breaches and ensure that the Reports are clarified in a transparent, efficient, and objective manner.

The internal reporting channel is introduced with the expectation that it will be used responsibly by all Reporting Persons and that it will only be used to report Breaches within the scope of this Policy.

1.3 Definitions

Whenever used in this Policy, the following terms shall have the following meaning:

Breach/es means a breach(es) of the applicable Romanian or European legislation in connection with or arising from the Company's activities which are illegal or unacceptable because they are contrary to the object or purpose of the rules in the acts of the EU (see section 3 below).

[1] Published in the Official Gazette of Romania, Part I, no. 1218 of 19 December 2022, as subsequently amended and supplemented.

[2] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, OJ L 305, dated 26.11.2019, p.17 -56.

Information on/about a Breach/es is information, including reasonable suspicion, about actual or potential Breaches that have occurred or are likely to occur at the Company or otherwise affecting the Company.

Report/s is/are report(s) of Information about (potential) Breaches to the Contact Persons.

Contact Person/s is/are the local person(s) responsible for handling Reports, including receiving and processing the submitted Reports, communicating with the Reporting Person and informing the Reporting Person about the actions taken in relation to the submitted Report. The Company's Contact Persons are set out in section 5 below.

Reporting Person/s is/are all person(s) who have obtained Information about Breaches during or in connection with the performance of their employment or work duties or in any other professional context.

Person/s Concerned is/are the natural or legal person(s) identified in the Report as the person(s) to whom the Breach is attributed or with which that Breach is associated.

Retaliation is any direct or indirect act or omission which occurs in a professional context, which is a reaction to a Report, or to any external report or public disclosure, and which causes or is likely to cause detriment to the Reporting Person or to third parties who are connected to the Reporting Person.

2. PROTECTION MEASURES

Regardless of whether the Reports are made under this Policy or under the procedures set in the IBM Group Policy, the persons who report Breaches honestly and in good faith are entitled to protection which includes **(i) keeping the Reporting Person's identity confidential and (ii) protection from acts of Retaliation**.

Confidentiality shall also be kept in terms of the identity of the Person(s) Concerned or other persons named in the Report.

With respect to Reports made under this Policy, the obligation to maintain confidentiality will not apply if state or local government authorities or competent courts demand the disclosure of certain information in compliance with the law. The Reporting Person will be informed in advance of the disclosure of their identity, unless the respective authority or court has informed the Company that notifying the person would jeopardise the relevant investigation, verification, or legal proceedings.

Reporting Persons who report Breaches under this Policy, will be **exempt from liability for obtaining, accessing, and disclosing the information**, unless obtaining or accessing the reported information constitutes a criminal or administrative offence. Reporting Persons will also not be held responsible for disclosure, provided that they have reasonable grounds to consider that the information is true and that the reporting is necessary to reveal the Breach.

The protection status extends to all facilitators and third party legal or natural persons connected to the Reporting Person and who may suffer Retaliation as a result of the Report.

3. BREACHES, WHICH REQUIRE REPORTS

Actual or potential Breaches of applicable laws of Romania and/or the EU, in the areas listed within Article 3 para. 1 of the Whistleblower Protection Law, **in or affecting the Company**, are to be reported through the internal reporting channel.

In particular, individuals should report under this Policy where they have Information about the following Breaches in or affecting the Company:

(a) Breaches of applicable legislation in the area of public procurement;

(b) Breaches of applicable legislation in the area financial services, prevention of money laundering and financing terrorism;

(c) Breaches of product safety regulations or other product-related regulations;

(d) Breaches of transport safety regulations;

(e) Breaches of applicable legislation in the area of protection of the environment;

(f) Breaches of radiation protection and nuclear safety regulations;

(g) Breaches of food and feed safety, animal health and welfare regulations;

(h) Breaches of public health regulations;

(i) Breaches of applicable legislation in the area of consumer protection;

(j) Breaches of privacy, personal data protection regulations, and network and information systems security;

(k) Breaches affecting the financial interests of the European Union, and breaches of internal market rules, including rules of European Union and Romanian legislation on competition and State aid;

(l) Breaches of corporate tax rules or arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

4. METHODS OF REPORTING

In the event of a violation of Romanian or EU law, in or affecting the Company, Reporting Persons can submit Reports in one or more of the following ways:

(i) via the internal reporting channel of the Company, or

(ii) to the National Integrity Agency (*in Romanian*: 'Agentia Nationala de Integritate', ANI), which acts as national external reporting office, at: Bucharest, 15 Lascăr Catargiu Bld., 010661, District 1, e-mail: avertizari@integritate.eu, telephone +40 372 069 869, website: avertizori.integritate.eu, or

(iii) by public disclosure of the Information about the Breach, subject to the conditions for doing so in the Whistleblower Protection Law.

Reporting Persons may choose to report in one way, a combination of two ways, or all three ways at the same time, with the observance of the legal provisions regarding public disclosure.

The Company encourages all employees and Reporting Persons to prioritise Reports **via the internal reporting channel** to ensure prompt and effective handling of Reports and prompt follow up by the Company.

5. IMPORTANT INFORMATION ON THE SUBMISSION OF A REPORT THROUGH THE INTERNAL CHANNEL

All Reporting Persons, whether they are part of the Company's structure or have received Information about a Breach in another work context, can submit written or verbal Reports by sending them to the Contact Persons and in the manner as specified in this section 5 of the Policy.

Reports must be submitted to the attention of any or all of the following local Contact Persons at the Company:

- **Fanel Enache**, CFO, Director, IBM Romania;
- **Cerasela Baiculescu**, Country Leader IBM Romania and Moldova;
- **Alexandra Buzoianu**, HR Leader - IBM Consulting CICs CEE.

Reports can be submitted to the Contact Persons **verbally** or **in writing**. At least one Contact Person will be available at all times, during working hours, to receive and process the Reports.

Reporting Person can submit a written Report by sending it to the Contact Persons:

(a) by email to the following email address: whistleblowingromania@ibm.com.

(b) by postal mail to the Company's address, as follows: *Bucharest, 15D Şoseaua Orhideelor, The Bridge, Building A, 5th floor, 060071, District 6*, marked 'CONFIDENTIAL', with a note on the envelope stating that the item is for the attention of the above Contact Persons or to any of them.

The Company's current employees may also submit written Reports via the Employee Concerns Program by completing the submission form, available on the following link: https://w3.ibm.com/hr/employee-concerns/#/home/employee-concerns. Reports for Breaches that fall within the scope of this Policy and are submitted via the Employee Concerns Program shall be transferred to the local Contact Persons to be reviewed under this Policy if the Reporting Person has provided his/her names and contact details. Anonymous Reports which are submitted via the Employee Concerns Program shall not be transferred to the local Contact Persons and/or processed under this Policy.

Reporting Person can submit a verbal Report either by telephone, or by arranging a personal or on-line meeting with the Contact Persons. For the purpose of submitting a verbal Report or arranging a meeting, Reporting persons may use any of the following telephone numbers:

- for Fanel Enache: +40 726 166 488
- for Cerasela Baiculescu: +40 731 790 480
- for Alexandra Buzoianu: +40 731 035 195

Reporting Persons who wish to remain anonymous may submit their Reports under this Policy by one, several or all of the following means: (i) anonymous postal mail, to the address provided above; (ii) anonymous telephone call; or (iii) e-mail, using a special purpose non-IBM e-mail address. **Please note that follow-up communication between the Contact Person(s) and the anonymous Reporting Person may only be maintained via e-mail or if other contact means are provided by the Reporting Person.**

Employees who have reason to believe that a conflict of interest would arise in the handling of a particular Report by all of the Contact Persons, may submit their Report to the Employee Concerns administrator at appeals@us.ibm.com or by phone at (914)499-4147 (USA). In this case, the Employee Concerns administrator shall process the Report in accordance with this Policy.

6. PROCESSING REPORTS

6.1 Responsibility for Processing of Reports

The Company's Contact Persons are responsible for receiving and handling Reports.

Contact Persons also performs other duties in accordance with their positions in the Company's structure. On a case-by-case basis, upon receipt of a Report, the Contact Persons shall ensure that the reconciliation of their other duties does not result in a conflict of interest. In the event of a suspected conflict of interest after receiving the Report, depending on the circumstances, the Report will be processed in accordance with this Policy by the other Contact Persons, by another person part of the Company's structure, with the approval of the Employee Concerns administrator, or by the Employee Concerns administrator.

Depending on the nature of the Report and the area in which it falls, persons from the IBM group structure (the "**Investigators**") may be involved in the verification of the information on the Report, subject to the requirements for ensuring the security and confidentiality of the information and the identity of the Reporting Person and other involved persons.

6.2 Submitting Reports

Persons who have Information about a Breach should submit a Report by one of the methods set forth in section 4 of this Policy, preferably through the Company's internal reporting channel.

Written Reports can be submitted at any time by using the methods of reporting set out in section 5 above.

Verbal Reports can be submitted during the established working hours of the Company. Where the Report is submitted verbally, subject to the prior consent of the Reporting Person, the Contact Persons shall document the Report either by:

(i) recording the conversation – in the case of reports received via telephone, the Contact Persons will request to arrange an on-line meeting via *Cisco Webex Meetings* or other appropriate on-line conferencing platform which allows for the recording of the conversion in safe conditions and in compliance with applicable data privacy regulations. If the Reporting Person wishes to remain anonymous, he/she may join the conference using a special purpose non-IBM e-mail address and without providing any identification details; or

(ii) complete and accurate transcription of the conversation. The Reporting Person shall be provided with the opportunity to review the transcription, make any comments or corrections, and sign the transcription minutes if they choose.

If the Reporting Person refuses to have the conversation recorded or transcribed, the Contact Persons will direct him/her to submit the Report in writing. Non-anonymous written Reports that are submitted via Employee Concerns program and fall within the scope of this Policy, shall be documented by the Contact Persons in the same manner as the verbal Reports.

Reports must always be complete, truthful, objective and unbiased, and contain sufficient specific information to allow verification.

Non-anonymous Reports must contain (i) the name and contact details of the Reporting Person, (ii) details regarding the professional context in which the information was obtained, (iii) the Person(s) concerned, if known to the Reporting Person, (iv) the description of the alleged Breach and (iv) the date and signature of the Reporting Person (for written Reports only).

Anonymous Reports must contain all information provided above, except for those listed under points (i) and (iv). **Please note that by submitting an anonymous Report without providing any valid contact details, you understand and agree that the Contact Person(s) will not be able to reach you, including for the purpose of requesting additional information. It is your responsibility to ensure that any such Report contains all information required for the analysis and resolution of the alleged Breach(es).**

In particular, the Report must contain specific details of the Breach or of a real risk of it being committed, the place and time of the Breach, a description of the act or the circumstances and such other circumstances that are known to the Reporting Person.

The Reporting Person may attach to the Report any type of information supporting the allegations made in the Report and/or documents, including reference to persons who could confirm the reported data or provide additional information.

All reports that are submitted through the internal channel and fall within the scope of this Policy shall be registered with the Register provided under section 7 of this Policy.

Reporting Persons who have provided valid contact details will receive confirmation of receipt of the Report from the Contact Persons within **seven days** of receipt at the latest.

6.3 Formal Verification of Reports

After receiving the Report, the Contact Persons shall check:

(a) whether the Report contains all the necessary information - the Contact Persons shall check whether the Report contains the required data in accordance with the Whistleblower Protection Law. Where irregularities are found and the Reporting Person has provided valid contact details, the Contact Persons shall, within seven days of receipt of the Report, send a notice to the Reporting Person to rectify them. If (i) the irregularities are not rectified within **fifteen days** as of receipt of the request at the latest, or (ii) an anonymous Report does not contain sufficient information for the analysis and resolution of the alleged Breach(es), the Contact Persons will dismiss the Report without further examination. Where possible, the Report, together with its annexes, shall be returned and the Reporting Person shall be notified in respect to the legal grounds for dismissal. Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns program.

(b) whether the Breach falls within the scope of this Policy - if the Breach referred to in the Report does not fall within the scope of section 3 of this Policy and the Reporting Person has provided valid contact details, the Contact Persons shall send a notice to the Reporting Person in which they return the Report and its attachments, stating the legal grounds and the reason why the Report will not be considered. Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns program. If the nature of the Report requires consideration by another competent authority, the Contact Persons may refer the Reporting Person to that authority.

(c) whether the Report is plausible and substantiated - the Contact Persons assesses whether the facts described in the Report are plausible in purely factual terms and whether the Report is substantiated by the claimed facts. Where the content of the Report does not support a finding that it is plausible and/or substantiated, or the reported Breach is manifestly a minor Breach, which requires no follow-up measures, the Contact Persons shall send a notice to the Reporting Person in which they return the Report and its attachments, stating the reason why the Report will not be considered (if the Reporting Person has provided valid contact details). Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns program.

Where the Report contains clearly false or misleading statements, it shall be returned to the Reporting Person with instructions to correct the statements and to inform them of the responsibility for allegations.

When a Report is returned in the above-mentioned cases, the Contact Persons shall return an e-mail, if such was provided by the Reporting Person, and document internally the date of receipt of the Report and the date and legal ground for its return/ dismissal.

Multiple Reports with the same object, originating from the same Reporting Person, will be joined together and the Reporting Person will be issued one confirmation notice in accordance with section 6.2. If subsequently, the Reporting Person submits further Reports with the same object, without providing any relevant additional information, such Reports shall be dismissed without further examination and returned to the Reporting Person, where possible.

6.4 Investigating the Facts

If the Report is plausible and substantiated, and there is no ground to dismiss/ return it to the Reporting Person, the Contact Persons or the Investigators proceed with an investigation of the facts stated in the Report.

The aim of the investigation is to determine whether or not the (possible) Breaches addressed by a Report exist.

For this purpose, the Contact Persons and the Investigators are entitled to contact the Reporting Person and the other persons, named in the Report, and - if necessary - conduct interviews with them and request and inspect necessary documents.

Investigations are conducted in an objective and impartial manner under the presumption of innocence.

The Person Concerned will be informed that they are the subject of an investigation and of their rights as a Person Concerned, and of their rights under data protection legislation applicable in Romania and under this Policy.

In the course of the investigation, the Contact Persons or the Investigators:

(a) will hear the Person Concerned and/or accept their written explanations;

(b) will collect and evaluate the evidence referred to by the Person Concerned;

(c) will provide the Person Concerned with all the evidence collected and will give them the opportunity to object to it, while preserving the confidentiality of the identity and ensuring the protection of the Reporting Person;

(d) will give the Person Concerned the opportunity to submit and identify new evidence to be collected in the course of the investigation.

The Contact Persons and the Investigators shall take into account all findings and collected evidence when assessing the facts of the case and deciding on follow-up measures.

The Contact Persons and the Investigators can obtain support in the investigation from other persons who are part of the Company's structure or who are employees of another company – part of IBM group, as well as obtain external support (e.g. by lawyers, auditors, other experts) provided that the confidentiality requirements are observed and if it seems appropriate and necessary to adequately clarify the facts.

No later than **three months** of the acknowledgement of receipt of the Report, the Contact Persons shall provide feedback to the Reporting Person on the action taken in relation to the Report received. The information shall be provided irrespective of whether the investigation has been completed or is still ongoing. Until the case is closed and follow-up measures are implemented, the Reporting Person must be kept informed whenever developments are recorded, except for the case where such information would jeopardize the investigation and/or implementation of follow-up measures.

6.5 Completion of the investigation

The Contact Persons and the Investigators will complete the investigation when:

(a) there is sufficient confirmation of the facts to be able to reliably assess that the (possible) Breach addressed by a Report does not exist/was not committed, or

(b) there is sufficient confirmation of the facts to be able to reliably assess that the (possible) Breach addressed by a Report exists, or

(c) further clarification of the facts by reasonable means seems impossible or unjustified.

Upon completion of the investigation, the Contact Persons shall document the results of the completed investigation as per the provisions of this Policy and adopt one of the following measures:

(a) to terminate the procedure for processing the Report in cases where:

  (i) it is established that the Breach referred to in the Report does not exist;

  (ii) further clarification of the facts by reasonable means seems impossible or unjustified;

  (iii) following the investigation, it is determined that the reported Breach is minor and does not require follow-up action;

(iv) the Report is about a Breach for which an investigation has already been conducted and completed by the Contact Persons or the Investigators and the resubmitted Report does not contain new information relevant to the Breach alleged in the Report;

(v) inform the statutory directors of the Company as per section 6.6 where evidence of a potential criminal offence is established, in which case the Company may notify the competent criminal bodies, as per the provisions of the applicable laws and internal Company policies.

(b) to take or arrange for specific follow-up measures to be taken to stop or prevent the Breach in cases where it has been detected or there is a real risk of such being committed. The Contact Persons may require the assistance of other persons or units within the structure of the Company. This right of the Contact Persons may be exercised in combination with the proposal to the Company to take specific measures and insofar as the functions performed by the Contact Persons allow it.

If the facts stated in the Report are confirmed, the Contact Persons may also refer the Reporting Person to the competent authorities if the nature of the Report requires consideration by another competent authority.

6.6 Information on the Results of the Investigation

Upon completion of the investigation, the Contact Persons shall provide a written report to the statutory directors of the Company, informing them of the result of the investigation, the actions taken and the follow-up actions immediately taken or to be taken to stop or prevent the Breach. The Reporting Person and the Person Concerned shall also be informed of the result of the investigation, by observing their rights hereunder.

In case of a conflict of interest with any of the statutory directors, depending on the circumstances, the report on the results of the investigation may be issued to the other statutory director or to another person acting as a representative of the Company. In such case, the recipient may also undertake any required actions based on such report.

The assessment of the existence of a conflict of interest shall be made on a case-by-case basis and in each of these cases, the Contact Persons and persons responsible for any follow-up actions shall strictly monitor compliance with the confidentiality requirement.

6.7 Analysis and Follow-up Measures

After the investigation has been completed, the Contact Persons will check whether the Report or the information obtained in the course of the investigation has revealed deficits or weaknesses in the Company's procedures and processes and propose appropriate measures to the Company's management.

The Company, through its designees, shall implement the specific follow-up actions and measures required to stop or prevent the Breach, and shall incorporate the information received with a view to improve the Company's procedures and processes.

6.8 Data Protection

If personal data are processed in the course of processing the Reports, this will be done in compliance with the provisions of the General Data Protection Regulation ("**GDPR**")[3] and Law no. 190/2018 on the implementation of GDPR ("**Law 190/2018**")[4].

The legal basis for processing personal data when handling Reports are:

- Where reporting Breaches of the law is concerned, the Company is obliged to process this data in accordance with Art. 6 (1) c) of the GDPR.
- Where processing other Reports is concerned, the legal basis is Art. 6 (1) f) of the GDPR; the Company has a legitimate interest in maintaining its reputation and ensuring compliance with its rules and policies.

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Promulgated, Official Journal of the EU 04.05.2016, L 119, p. 1- 88.

[4] Published in the Official Gazette of Romania, Part I, no. 651 of 26 July 2018, as subsequently amended and supplemented.

Personal data that are clearly not relevant to the consideration of the specific Report shall not be collected and, if accidentally collected, shall be deleted.

7. RECORD OF THE REPORTS AND STATISTICS

The Company shall establish and approve a template Register of the Reports of Information on Breaches (the "**Register**"). The Company, through the Reporting Persons, shall also keep statistics in respect of the reported Breaches, including (i) annual number of received Reports via the internal reporting channel, including number of nominal and anonymous Reports; (ii) undertaken measures (i.e., Reports dismissed without further examination/ returned to the Reporting party, Reports referred to further investigation, Reports closed under one of the grounds provided at section 6.5); (iii) established Breaches; (iv) follow-up measures; and (v) value of damage incurred by the Company as a result of the established Breaches/ value of damage recovered (where the case). Internal documents containing statistics shall be kept strictly confidential and shall be presented only to the directors of the Company, or to other persons from the Company structure, on a need-to-know basis, as well as to the National Integrity Agency, upon request.

7.1 Procedure for Keeping and Maintenance of the Register

The Register is kept and maintained by the Contact Persons. The Register must reflect the following information: (i) date of Report receipt; (ii) name and contact information of the Reporting Person (where known); (iii) object of the Report; and (iv) resolution provided to the Report as per section 6.5.

The Register is not public. The Register shall be created, maintained, and stored in electronic form with controlled access. Only the Contact Persons shall have access to the Register through individual username and password. Access to the information in the Register may exceptionally be granted to other persons who, in accordance with the Whistleblower Protection Law and the regulations adopted thereunder, are expressly authorised with the right of access.

7.2 Obligations of the Contact Persons with regard to the Register

The Contact Persons are required to register in the Register all Reports that are received through the internal reporting channel and that fall within the scope of the Whistleblower Protection Law.

When completing the information in the Register, the Contact Persons are obliged to correctly enter all data from the received Report, to monitor for inconsistencies and missing data in the Report and to take the necessary actions for their timely removal and clarification.

The Contact Persons shall take and comply with all technical and organisational measures specified in section 8 to ensure the confidentiality and security of the information in the Register.

8. STORING OF REPORTS. TECHNICAL AND ORGANISATIONAL MEASURE TO ENSURE THE CONFIDENTIALITY AND SECURITY OF THE INFORMATION FROM THE REPORTS REVEIVED

The Reports, as well as any and all documents and information in relation thereto, as well as the information on any and all actions taken by the Contacts Persons, or by the Company, and the information in the Register shall be stored on a durable medium (paper and/or an electronic carrier) for a period of 5 (five) years from the date of completion of the actions under the Report, unless otherwise specified by law. Upon expiry of the storage period, the Report and any supporting documents/ attachments thereof, regardless of their support, shall be destroyed.

8.1 Hard copy Reports and Documents

Reports, documents and information, received on hard copy shall be stored in the Company's premises.

The Company shall take the following technical and organisational measures to ensure the confidentiality and security of the submitted hard copy Reports, documents and information:

8.1.1 Reports and documents shall be stored in special locked cabinets accessible only by the Contact Persons.

8.1.2 Reports and documents shall not be moved outside the Company's premises except when it is necessary to forward them to a competent authority or return them to the Reporting Person.

8.1.3 The Contact Persons may create electronic copies of submitted hard copy Reports and documents, which shall be stored in accordance with section 8.2 below.

8.1.4 The Company's premises where the hard copy Reports and documents are stored are subject to 24/7 physical and/or technical security (through signalling and security technology and video surveillance) and implemented procedures for control of the physical access.

8.2 **Electronic Reports and Documents**

Reports that are submitted electronically and the documents in relation thereto are stored in conditions of proper security, on a server, in shared folders with restricted access.

The Company shall take the following technical and organizational measures to ensure the confidentiality and security of electronically submitted Reports and the documents in relation thereto:

8.2.1 Only the Contact Persons have direct access to the folders in which the electronic Reports and the documents in relation thereto are stored, through individual usernames and passwords (known to each of them only, respectively).

8.2.2 Where necessary the Contact Persons can grant limited and restricted by time access to a specific case file to third persons, by strictly observing the rules therefore under this Policy.

IBM ROMANIA S.R.L.