WHISTLEBLOWER POLICY

Effective Date: February 23, 2021

1. Scope

B2Gold Corp. ("**B2Gold**" and together with its subsidiaries, affiliates, joint ventures and any other entity controlled by B2Gold, the "**B2Gold Group**") will make available to all of its directors, officers, employees, consultants and contractors of the B2Gold Group and, as appropriate, to third parties, (collectively, "**B2Gold Personnel**") procedures to enable the communication of "whistleblower incidents" (as defined under Section 3 below).

2. Purpose

B2Gold is committed to the highest possible standards of ethical and legal business conduct. In line with this commitment and B2Gold's commitment to open communication, this policy aims to provide an avenue for B2Gold Personnel to raise concerns and reassurance that B2Gold Personnel will be protected from reprisals or victimization for whistleblowing in good faith.

The Executive VP, General Counsel & Secretary of B2Gold has been designated as the individual responsible to oversee this policy.

3. Defined Terms

Whistleblower Incident

A "**whistleblower incident**" is defined as a concern related to the B2Gold Group's accounting, internal accounting controls and auditing matters, a violation of B2Gold's Anti-Corruption Policy or compliance with applicable laws.

The whistleblowing procedure is intended to be used for potentially serious and sensitive issues. For greater clarity, whistleblower incidents are intended to include, but are not limited to the following:

- Deficiencies in or lack of compliance with internal accounting controls;
- Any fraud or deliberate error in preparing, evaluating, reviewing or auditing any of the B2Gold Group's financial statements;
- Inappropriate revenue recognition;
- Inappropriate capitalization of assets;
- Inappropriate recognition of B2Gold Group liabilities (e.g. environmental clean-up costs);

- Embezzlement of B2Gold Group assets by an individual or group of individuals; and
- Misrepresentation of non-financial information to support the financial statements.

As outlined in the above definition, whistleblower incidents relate primarily to matters regarding the B2Gold Group's accounting, internal accounting controls or auditing, violations of B2Gold's Anti-Corruption Policy or compliance with applicable laws. As such, whistleblower incidents are **NOT** intended to include such matters as:

- "Routine" grievances on operational matters of the B2Gold Group;
- Harassment; and
- Discrimination.

Please refer to other appropriate B2Gold Group policies and procedures dealing with such incidents. Employment-related concerns should continue to be reported through your normal channels, such as your supervisor, local HR representative, or to the Chairman of the Board of Directors of B2Gold (the "**Board**"), pursuant to the applicable B2Gold Group policy.

4. Policy and Policy Statements

This whistleblowing policy is intended to cover serious concerns that could have a significant impact on the B2Gold Group, such as actions that:

- May lead to incorrect financial reporting;
- Are unlawful; or
- Otherwise amount to serious improper conduct.

It is the policy of the B2Gold Group that all B2Gold Personnel must immediately report whistleblower incidents as soon as the B2Gold Personnel becomes aware of such situations.

Whistleblower incidents shall be reported using the B2Gold Group's prescribed procedures for the submission of whistleblower incidents (*see Section 5.2 below*).

4.1. Harassment or Victimization

It is the policy of B2Gold that B2Gold Personnel will not be discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated or retaliated against as a result of communicating a whistleblower incident in good faith or providing assistance to the Audit Committee of the Board (the "**Audit Committee**"), management or any other person or group in connection with a whistleblower concern, including any investigation by a governmental, regulatory or law enforcement body. A "good faith" report is one which is made honestly and reasonably, whether or not the person has all of the relevant facts or is sure that a breach has occurred. Any B2Gold Personnel who retaliates against someone who has made a report in good faith will be subject to

discipline up to and including termination of their employment or consulting arrangement.

4.2. Confidentiality

It is the policy of B2Gold to treat all reported whistleblower incidents in a confidential and sensitive manner to the fullest extent possible, consistent with applicable law and the need to conduct an appropriate review. *See Section 6 below*.

4.3. Anonymous Allegations

The policy encourages B2Gold Personnel to put their names to allegations because appropriate follow-up questions and investigation may not be possible unless the source of the information is identified. Concerns expressed anonymously will be investigated, but consideration will be given to:

- The seriousness of the issue raised;
- The credibility of the concern; and
- The likelihood of confirming the allegation from attributable sources.

4.4. Malicious Allegations

Malicious allegations (allegations not made in good faith) may result in disciplinary action.

5. Procedure

5.1. Process For Raising A Concern

As a first step, we encourage B2Gold Personnel to report any known violations or complaints to their immediate supervisor or to the persons set out below. If they do not feel comfortable reporting the information to their immediate supervisor or to the persons set out in Section 5.2 below, then B2Gold Personnel may report the information to Whistleblower Security Inc., a third party service provider ("**Whistleblower Security**").

Whistleblower Security has been contracted by B2Gold to facilitate any concerns. Whistleblower Security serves as an avenue for disclosure of illegal activities as observed or witnessed by B2Gold Personnel. Whistleblower Security offers 24/7 access to confidential methods of disclosing these activities. We encourage open dialogue within the B2Gold Group, but if you feel it necessary, please follow the procedures as detailed below to help retain the integrity of our workplace.

5.2. Reporting

Whistleblower incidents should be reported in any of the following ways:

- Through the Hotline: North America: 1-866-921-6714
- Contacting either of the following:

  Robert Gayton, Chairman of the Audit Committee at or rgayton@b2gold.com

  Robert Cross, Chairman of the Board at bcross@b2gold.com

- If you are not in North America, call collect to 1-604-921-6875 during business hours and say you are with B2Gold and have a whistleblower report
- Through the web form at www.whistleblowersecurity.com (see Appendix "A" attached for a sample of the web form)
- Email B2Gold@whistleblowersecurity.com
- Fax report to: 1-604-926-5668
- Mailing address alternative for written documents: Suite 300 - 1455 Bellevue Avenue, West Vancouver, British Columbia, Canada V7T 1C3

5.3. Document Retention

The Audit Committee, or its designee, will retain a copy of the summary logs, all submitted complaints and concerns and all substantive documents provided or generated pursuant to any investigation hereunder for a period of not less than five years.

6. Confidentiality

Confidentiality of complaints received, whether anonymously or otherwise, will be maintained to the fullest extent possible, consistent with applicable law and the need to conduct an appropriate review.

Whistleblower Security or the person to whom the incident is reported pursuant to this policy will take the initial report from the individual and notify the appropriate B2Gold Group representative, which is the Chairman of the Audit Committee (or other appropriate person as determined by the Audit Committee). Whistleblower Security will act as the communication liaison between the person reporting the alleged matter and the B2Gold Group to safeguard the anonymity and confidentiality of the reporter. The B2Gold Group will not have access to your name if you choose to share it with Whistleblower Security during the course of your report, unless you specifically authorize it.

7. Timing

The earlier a concern is expressed, the easier it is to take action.

8. Evidence

Although the individual is not expected to prove the truth of an allegation, the individual needs to demonstrate to the person contacted that there are sufficient grounds for concern.

9. How The Complaint Will Be Handled

The action taken will depend on the nature of the concern. The Audit Committee and the Board will receive a report on each complaint from the Chairman of the Audit Committee (or any other appropriate person as determined by the Audit Committee). The Audit Committee or its designee will oversee the investigation and resolution of any reported incidents that present a material issue, as determined by the Audit Committee. The Audit Committee has the authority to retain outside legal or accounting expertise in any investigation as it deems necessary to conduct the investigation in accordance with its charter and this policy. Notwithstanding the foregoing, in no event will a member of the Audit Committee or its designee be involved in any aspect of the investigation or resolution of a report if the report alleges that he or she was involved in the matter.

10. Initial Inquiries

Initial inquiries will be made to determine whether an investigation is appropriate, and the form that it should take. Some concerns may be resolved by agreed action without the need for investigation.

11. Report to Complainant

Subject to any requirements of confidentiality, whether reported to B2Gold Personnel or through Whistleblower Security, the complainant will be given the opportunity to receive follow-up on their concern in two weeks acknowledging that the concern was received and, where possible and when determined to be appropriate by the Chairman of the Audit Committee or the Audit Committee:

- Indicating how the matter will be dealt with;
- Giving an estimate of the time that it will take for a final response;
- Telling them whether initial inquiries have been made; and
- Telling them whether further investigations will follow, and if not, why not.

In addition, when reporting an incident the complainant will be provided with a password. The complainant may check back with Whistleblower Security at any time and check on the status of the claim by using the password provided.

12. Further Information

The amount of contact between the complainant and the body investigating the concern will depend on the nature of the issue and the clarity of information provided. Further information may be sought from the complainant.

13. Resolution

Please be aware that during the course of the investigation, you may not know that the B2Gold Group is taking action. Due to the confidential nature of some disclosures, investigations may be required to be conducted privately and cautiously.

14. Information

Subject to legal constraints the complainant will receive information about the outcome of any investigations.

15. Compliance

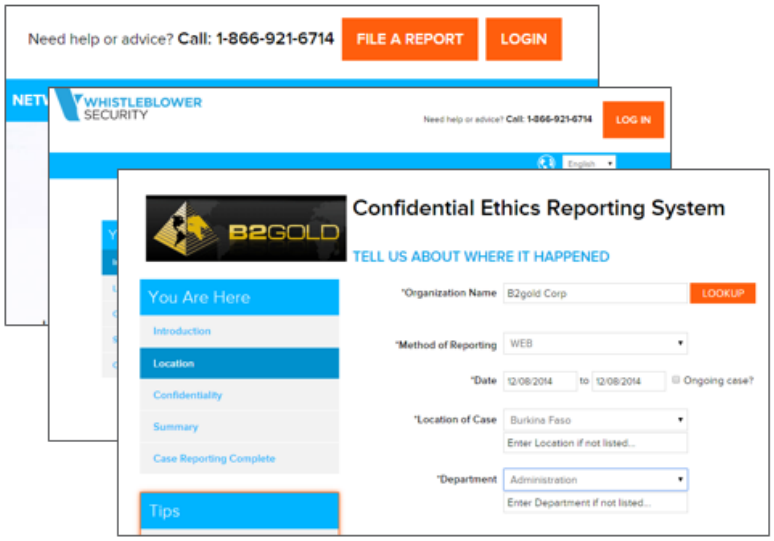
B2Gold Personnel are expected to read and become familiar with this policy when they begin their engagement with the B2Gold Group and may be required, from time to time, to affirm in writing their compliance with this policy.

B2Gold appreciates your support and diligence in creating a better work environment for us all. If you have any questions about this policy, please contact Mr. Roger Richer, Executive VP, General Counsel & Secretary or Mr. Mike Cinnamond, Senior VP Finance & Chief Financial Officer at B2Gold's Head Office in Vancouver, British Columbia.

B2Gold ***reserves the right to modify or amend this policy at any time as it may deem necessary.***

APPENDIX "A"

Navigate to www.whistleblowersecurity.com and click on **File a Report**. This will take you to the Confidential Ethics Reporting System page advising you of the process, your anonymity and the obligations present for all parties. Read through the terms of service and then check the "I agree" box to agree to the terms of service and then select Continue.

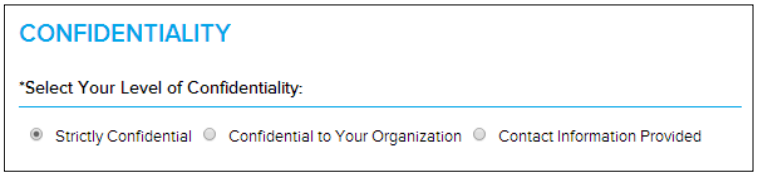


The next screen is **Location,** where you will provide details about where your incident took place. The information you will provide is:

- **Organization Name** – type the first few letter of your organization's name, hit lookup, choose your organization
- **Method of Reporting** – make sure you choose "web" in the organization's drop down menu
- **Case Date** – choose your incident date
- **Location of the Case** – choose the location where the incident took place from the drop down menu
- **Department** – choose the department involved in the case from the drop down menu

When you're ready to keep going, click **Continue**

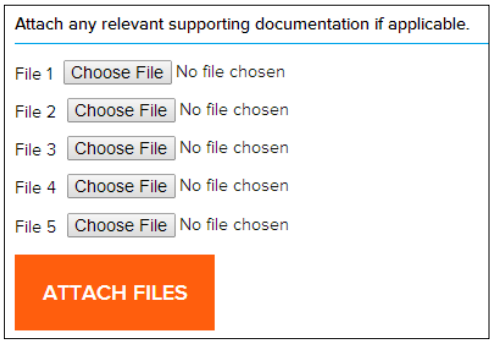
You have now reached the **Confidentiality** section. You will see there are three levels of confidentiality. You can select any one of these – the choice is yours:



- **Strictly Confidential** – gives you the highest level of anonymity and protection. If you select this option, your identity will not be known by either your organization or to WhistleBlower Security. In this case, you are completely confidential.

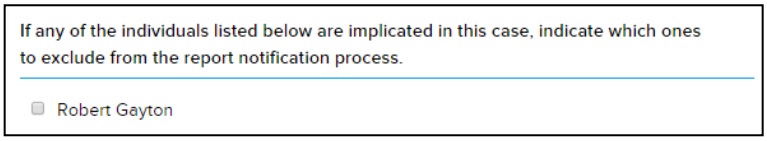
- **Confidential to your Organization** – by selecting this option, the system will share your information with WhistleBlower Security only, but not with your organization.

- **Contact Information Provided** – when you select this option, both your organization and WhistleBlower Security will be notified about your incident. This means that your organization might have a representative contact you directly to resolve the issue.

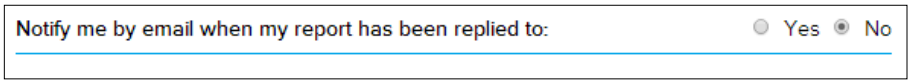


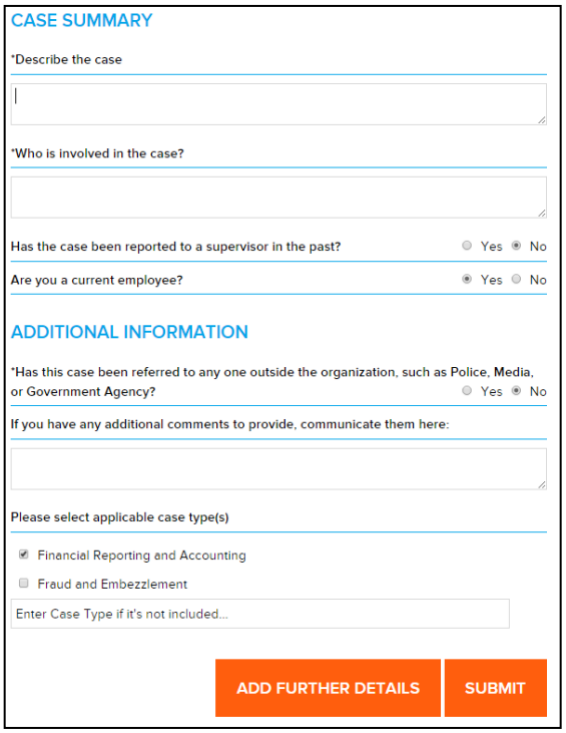
Do you have any relevant supporting documentation? You can choose your files here by clicking “Choose File” to retrieve your document(s). Don’t have anything? Simply skip this section.

Next is the list of designated individuals from your organization who will be included in your incident report notification. If any of these individuals are implicated in your case and you do not want them to be notified of your incident, you can choose to remove them from the process by checking the box next to their name.



Would you like to be notified by email when your incident report has been replied to through the system? You can make your choice here by clicking Yes or No.





The next section is Case Summary. This where you will describe your incident and list who is involved in the case. You can type as freely as you wish here, in your own words. Type as little or as much as you like.

You can indicate if the case has been reported to a supervisor in the past.

You can indicate if you are a current employee or not.

You can indicate if your case has been referred to anyone outside your organization such as the police, media, or a government agency.

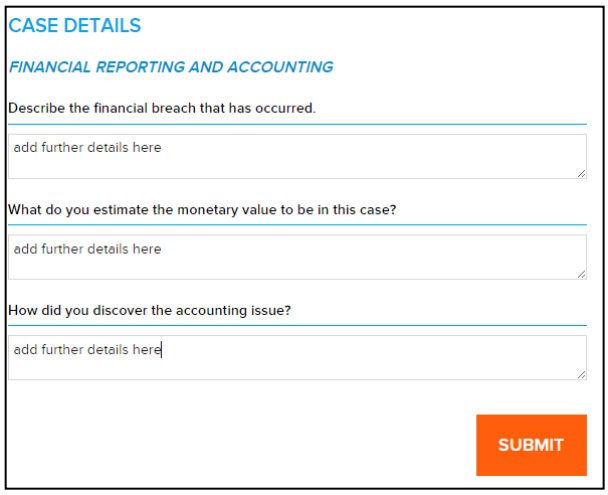
Any additional comments can be added in this section also.

Before you continue, you must select the applicable Case Type. You can choose up to three and if you don't see your Case Type listed here, you can add it in to the box provided at the bottom.

Here, you have the choice to either submit your incident, or add in any additional information to support your case.

If you choose to add further details, you will be taken to a section where you can further describe the details of your case. The questions you see in this section are dependent on what Case Type(s) you checked off previously.

Once you have finished further describing your case, you can click the **Submit** button.



Your incident has now been submitted and your case reporting is complete. The details you have provided will be captured for review by your organization's designated auditors. You will be presented with an Incident **ID Case Number**, **Login Name**, and **Password** for the system.

Take a moment to write this information down so you can retrieve it later. Once you have left this page you are unable to return. Log in anytime to view and/or print your incident or add future details and correspond directly with your organization's representatives.

CASE REPORTING COMPLETE

Thank you for submitting a report through the WhistleBlower Security system. You can now review your report and have the opportunity to provide additional information or pose comments or questions to the Management Team.

If you have not provided your email address, please log back into the site within 48-72 hours to see if the organization has responded to your report and you will be able to review their response and make additional comments.

Incident ID

Login Name

Password