



WHISTLEBLOWER POLICY

Effective May 13, 2013
(as amended March 13, 2018)

1. Scope

B2Gold Corp. ("B2Gold" or the "Company") will make available to all of its officers and employees and, as appropriate, to third parties, procedures to enable the communication of "whistleblower incidents" (as defined under Section 3.2 below).

2. Purpose

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

3. Defined Terms

3.1 **The Company**

For the purpose of this policy the "Company" and "B2Gold" is meant to be B2Gold Corp. and includes all of its wholly-owned or partially-owned subsidiaries and joint ventures where B2Gold Corp. is the operator.

3.2 **Whistleblower Incident**

A "whistleblower incident" is defined as a concern related to the Company's accounting, internal accounting controls and auditing matters.

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 Company's financial statements;
- Inappropriate revenue recognition;
- Inappropriate capitalization of assets;
- Inappropriate recognition of Company liabilities (e.g. environmental clean-up costs);
- Embezzlement of Company 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 Company's accounting, internal accounting controls or auditing. As such, whistleblower incidents are **NOT** intended to include such matters as:

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

Please refer to other appropriate Company policies and procedures dealing with such incidents.

4. Policy and Policy Statements

This whistleblowing policy is intended to cover serious concerns that could have a large impact on B2Gold, 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 Company that an employee must immediately report **whistleblower incidents** as soon as the employee becomes aware of such situations.

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

4.1 Harassment or Victimization

It is the policy of the Company that employees 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**. 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.

4.2 Confidentiality

It is the policy of the Company to treat all reported incidents in a confidential and sensitive manner.

4.3 Anonymous Allegations

The policy encourages employees and third parties 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 our employees 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 below, then employees 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 our employees. Whistleblower Security offers 24/7 access to confidential methods of disclosing these activities. We encourage open dialogue within the Company, but if you feel it necessary, please follow the procedures as detailed below to help retain the integrity of our workplace.

5.2 Reporting

The whistleblowing procedure is intended to be used for serious and sensitive issues. Serious concerns relating to the **Company’s accounting, internal accounting controls or auditing matters and compliance with applicable laws** should be reported in either of the following ways:

- Through the Hotline: North America: 1-866-921-6714
- Contacting either of the following at B2Gold@whistleblowersecurity.com:
 - Robert Gavton. Chairman of the Audit Committee
 - Robert Cross, Chairman of the Board
- If you are not in North America, call collect to 1-604-921-6875 during business hours and say you are with B2Gold Corp. 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

Individuals reporting incidents will have the ability to remain anonymous if they choose. The Company will treat all disclosures in a confidential and sensitive manner. Whistleblower Security will take the initial report from the individual and notify the appropriate company representative, which is the Chairman of the Audit Committee or his designate. Whistleblower Security will act as the communication liaison between the person reporting the alleged matter and the Company to ensure the anonymity and confidentiality of the reporter. The Company 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.

Employment-related concerns should continue to be reported through your normal channels such as your supervisor, local HR representative, or to the Board Chairman.

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 of B2Gold and the Board of Directors will receive a report on each complaint. The Audit Committee or its designee will oversee the investigation and resolution of any reported incidents that present a material issue. 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 designate 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 Corp. 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;
- 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 company 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.



B2Gold Corp. 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 the Company's Head Office in Vancouver, British Columbia.

B2Gold Corp. 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 letters 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.

CONFIDENTIALITY

*Select Your Level of Confidentiality:

Strictly Confidential Confidential to Your Organization Contact Information Provided

Attach any relevant supporting documentation if applicable.

File 1 No file chosen
File 2 No file chosen
File 3 No file chosen
File 4 No file chosen
File 5 No file chosen

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.

If any of the individuals listed below are implicated in this case, indicate which ones to exclude from the report notification process.

Robert Gayton

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.

Notify me by email when my report has been replied to:

Yes No



CASE SUMMARY

*Describe the case

Who is involved in the case?

Has the case been reported to a supervisor in the past? Yes No

Are you a current employee? Yes No

ADDITIONAL INFORMATION

*Has this case been referred to any one outside the organization, such as Police, Media, or Government Agency? Yes No

If you have any additional comments to provide, communicate them here:

Please select applicable case type(s)

Financial Reporting and Accounting
 Fraud and Embezzlement

Enter Case Type if it's not included...

ADD FURTHER DETAILS **SUBMIT**

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.

CASE DETAILS

FINANCIAL REPORTING AND ACCOUNTING

Describe the financial breach that has occurred.

add further details here

What do you estimate the monetary value to be in this case?

add further details here

How did you discover the accounting issue?

add further details here

SUBMIT



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 **G-000000**

Login Name **W-000000**

Password **fr-000000**