IRMA

Initiative for Responsible Mining Assurance

EXCERPT FROM THE

IRMA Standard

for

Responsible Exploration, Extraction, and Processing of Minerals

2nd DRAFT

for public consultation

CHAPTER 3.4 – **Security Forces**

IRMA Standard v2.0 DRAFT 2

July 2025

English Version

Disclaimer and Context on this Draft

The 2nd DRAFT Version of the IRMA Standard for Responsible Exploration, Extraction, and Processing of Minerals V2.0 (hereafter referred to as the "2nd DRAFT") is being released for public consultation, inviting the world to join once again in a conversation around expectations that drive value for greater environmental and social responsibility in mining and mineral processing.

The 2nd DRAFT does not represent content that has yet been formally endorsed by IRMA's equally-governed multi-stakeholder Board of Directors. IRMA's Board leaders seek the wisdom and guidance of all readers to inform this through an inclusive revision process one more time, to improve the Standard.

This draft document builds on the 1st DRAFT Version published in October 2023, and invites a global conversation to improve and update the 2018 IRMA Standard for Responsible Mining V1.0. This 2nd DRAFT is intended to provide as final of a look-and-feel as possible, although input from this consultation will result in final edits, and consolidation to reduce overall number of requirements (more on this on page 6), for a version that will be presented to IRMA's equally-governed multi-stakeholder Board of Directors for adoption and implementation.

This 2nd DRAFT has been prepared and updated by the IRMA Secretariat based on:

- learnings from the implementation of the current IRMA Standard (V1.0)
- experience from the first mines independently audited (as of July 2025, 24 sites have completed audits or are in the process of being audited)
- evolving expectations for best practices in mining to reduce harm
- comments and recommendations received from stakeholders and Indigenous rights-holders
- the input of subject-specific Expert Working Groups convened by IRMA between 2022 and 2024
- all comments and contributions received during the public-comment period of the 1st DRAFT version (October 2023-March 2024)

Please note that Expert Working Groups were created to catalyze suggestions for solutions on issues we knew most needed attention in this update process. They were not tasked to come to consensus nor make formal recommendations. Their expertise has made this consultation document wiser and more focused, but work still lies ahead to resolve challenging issues. We encourage all readers to share perspectives to improve how the IRMA system can serve as a tool to promote greater environmental and social responsibility, and create value for improved practices, where exploration, extraction, and processing of minerals happens.

IRMA is dedicated to a participatory process including public consultation with a wide range of affected people globally and seeks feedback, comments, questions, and recommendations for improvement of this Standard. IRMA believes that diverse participation and input is a crucial and determining factor in the effectiveness of a Standard that is used to improve environmental and social performance in a sector. To this end, every submission received will be reviewed and considered.

This current 2nd DRAFT is based on content already in practice in the IRMA Standard for Responsible Mining V1.0 (2018) for mines in production, and its accompanying normative Guidance document and Supplementary Guidance, combined with the content drafted in the IRMA Standard for Responsible Mineral Development and Exploration ('IRMA-Ready' Standard – Draft v1.0 December 2021) and in the IRMA Standard for Responsible Minerals Processing (Draft v1.0 June 2021), and offers an updated version of the 1st DRAFT Version of the IRMA Standard V2.0 that received over 2,500 unique points of comments between 2023 and 2024.

Please note: The IRMA Standard V2.0 is new in its approach in that it now covers more phases of the mining and mineral supply chain, from exploration and development, through mining, closure, and mineral processing. IRMA also, separately, oversees a Chain of Custody Standard for tracking materials through the supply chain from mine-to-market end use products.

Disclaimer on Language and Corrections

For this public consultation, only an English version is available. A Glossary of Terms used in this Standard is provided at the end of the full version of the document (see below). IRMA reserves the right to publish corrigenda on its web page, and readers of this document should consult the corresponding web page for corrections or clarifications.

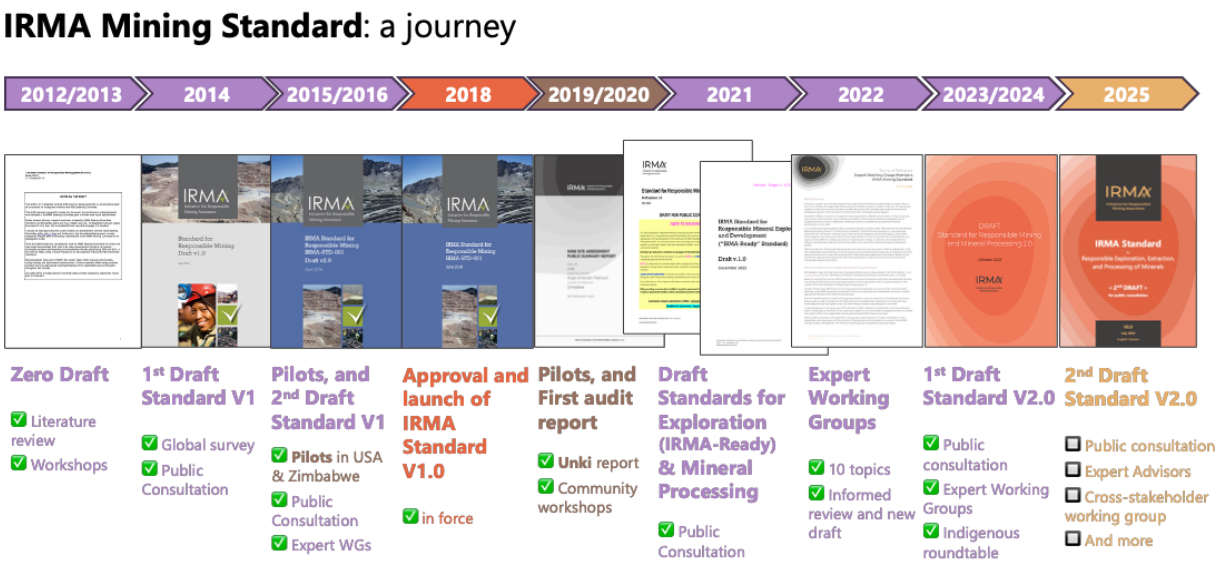
This document provides only one chapter excerpt from the IRMA Standard v2.0 DRAFT 2.

The full version contains 27 Chapters, click here to view it.

Objectives of this 2nd public consultation

Following the release of a 1st DRAFT of the IRMA Standard V2.0 in October 2023 for a 90-day public consultation, the IRMA Secretariat received more than 2,500 points of comments from 82 organizations, then organized additional engagement with stakeholders and Indigenous rights-holders, and solicited complementary guidance from multiple topic-specific Expert Working Groups.

We anticipated release of this 2nd DRAFT for a second round of public consultation as early as Q3 2024, then subsequently announced that more time was needed to support engagement of diverse stakeholders; the revised release date was July 2025. We provided more detailed explanation for the extended process here and here.



The release of this 2nd DRAFT marks a significant milestone on the road to the revision of the IRMA Standard: this public consultation will be the last of this revision cycle on V2.0.

Informed by the outcomes of this public consultation, along with guidance from Expert Advisors and IRMA Working Groups (see more below), and additional engagement with Indigenous rights-holders and stakeholders as requested, the IRMA Secretariat will prepare a final version. This final version will be discussed by the IRMA Board and refined to reach consensus for adoption by all six governing houses of IRMA: Affected Communities including Indigenous Rightsholders; Environmental and Social NGOs; Organized Labor; Finance and Investment Professionals; Mining Companies; Purchasers of Mined Materials.

In IRMA's strategic decision-making, Board members work to achieve consensus. IRMA believes a majority vote is not a model of equal governance. Instead, any motion that results in both of the two representatives from the same governing house voting "no" must go back to the full group for further discussion. In other words, a proposed course of action cannot proceed if both representatives from one of our six governing houses are opposed. Board members will keep talking until a resolution that works for all groups is found. It is a model that has worked for IRMA for nearly two decades and is fundamental to IRMA's credibility, accountability and service to all six houses of governance.

What is IRMA seeking guidance on?

Comments, feedback, and suggestions are welcome on any aspect of this 2nd DRAFT version (including intent and text of the requirements, endnotes, annexes, format and structure, design, readability, etc.).

IRMA is particularly interested in hearing the views of rights-holders and stakeholders on **the provisions in the Standard that are substantially new compared to the IRMA Standard for Responsible Mining V1.0.** These provisions (requirements or at a sub-requirement level) are highlighted in yellow throughout this Draft, to ensure they are easily identifiable.

We ask readers to assist us in weighing these potential new provisions, and also hold awareness that, prior to adoption of the final version, many of these will be consolidated and reduced in overall number.

Although these new requirements have each been drafted in response to lessons learned, the current state of best practices, emerging expectations, and/or in response to requests and suggestions made during the previous public consultation, collectively they represent substantive increased expectations for both implementing entities and audit firms. The IRMA Board of Directors seeks to ensure that the IRMA Standard, while recognized the world's most rigorous and comprehensive mining standard, continue to welcome and support uptake of newcomer companies engaging from the mineral supply chain around the world.

Thus, in this consultation, we seek guidance from all on **the new provisions that seem most urgent** to be integrated in the final version of the Standard V2.0, so that the revised Standard's expectations are paced at a realistic level to support engagement of mineral operations of a range of sizes, materials and global contexts.

It is important to note that all new requirements and sub-requirements, including those not retained in the final V2.0, will serve as the basis for the ongoing review process once the V2.0 is approved and released by our Board, and will provide fodder for future revisions, when it is decided that a V2.1 or V3.0 is needed.

Chapter 3.4
Security Forces

SECOND DRAFT (JULY 2025): SUMMARY OF CHANGES

- Chapter renamed 'Security Forces' since security arrangements are only a sub-part of this Chapter.
- Increased clarity and details for requirements related to selection and vetting, and training, in line with the International Code of Conduct for Private Security Providers, and the 2023 DCAF-ICRC Security and Human Rights Toolkit.
- Added requirements to clarify the content and nature of the monitoring and evaluation and continuous improvement corrective measures/updates (Sections 3.4.9 and 3.4.10)
- Added requirements to clarity the content of the annual reporting on security management (Section 3.4.11).
- Added one optional IRMA+ requirement to collaborate with other relevant stakeholders (i.e. other than affected people) including civil society, human rights experts, security providers, representatives of the country of operation's government, and other companies to share lessons learned and address challenges in the management of security risks and impacts (3.4.7.4).
- Substantial structural changes to increase clarity and consistency with the rest of the Standard.

RESPONSE TO CONSULTATION QUESTIONS OUTLINED IN FIRST DRAFT

Question #	Question	Feedback and Decision
1.4-02	**(3.5.6.3 – specific grievance mechanism; repat from Chapter 1.4 (now 1.6))** Background: Chapter 1.4 - 'Complaints and Grievance Mechanism and Access to Remedy' includes a range of requirements surrounding the existence of an accessible and effective operational-level grievance mechanism. It is not possible to score well on Chapter 1.4 if the mechanism does not have certain quality-related characteristics. Other chapters (i.e., human rights, gender, resettlement, security, ASM) also have requirements relating to the existence of a grievance mechanism; however, the requirements in each of those chapters ask only that a mechanism is in place that allows grievances to be filed and addressed, but they do not speak to the overall quality of that mechanism. This is an approach proposed by IRMA to avoid too much repetition across chapters. However, this creates a situation in which an ENTITY could theoretically score 'fully meets' on the grievance-related requirement in an individual chapter (which in most cases only asks that stakeholders have "access to" a grievance mechanism), even if the grievance mechanism as a whole is not an effective one (as reflected in the overall score for Chapter 1.4). Question: Should an ENTITY's score on grievance-related **requirements** within individual non-grievance-specific chapters be restrained or linked to the overall score that the ENTITY gets on the grievance chapter (Chapter 1.4) as a whole? For example, if a site scores 80% on Chapter 1.4, the most the site could receive for a grievance requirement in the other chapters would be a 'substantially meets,' but if a site scores 100% on Chapter 1.4 then, assuming the mechanism can handle grievances specific to the other chapters, they could possibly get a 'fully meets' rating on those grievance requirements.	**Feedback received**: Feedback largely supported putting a 'cap' on the ENTITY's score on grievance-related mechanisms in other chapters based on its performance on Chapter 1.6 (former 1.4). **Decision**: The Scoring system is adjusted to ensure that an ENTITY's potential score on the grievance-related requirement in an individual chapter (which simply requires the existence of a grievance mechanism capable of receiving grievances relating to the particular issue, or in Chapter 2.2 that mechanism/s are specifically designed with, and for, Indigenous Peoples) is limited by their score on Chapter 1.6 (former 1.4) on Grievances (which addresses not just the existence but also the quality of a grievance mechanism). This means that, although an ENTITY may have otherwise received 'fully meets' on a grievance mechanism requirement in an issue-specific chapter, if the ENTITY does not receive a full score on Chapter 1.6 as a whole, then their score on the issue-specific grievance requirement cannot be higher than 'partially meets'. If the ENTITY has developed separate issue-specific grievance mechanism/s, it will be assessed separately against all relevant requirements of Chapter 1.6.

BACKGROUND

Security risks to mining and mineral processing operations may result from political, economic, civil, or social factors. The role of private and public security forces used in relation to such operations should be to maintain the rule of law, including safeguarding human rights; provide security to workers, equipment, and facilities; and protect the site or transportation routes from interference with legitimate extraction and trade.

Security arrangements for mining and mineral processing operations that are founded on a substantial understanding of the context, consultation with stakeholders, and adherence to international best practice can help an ENTITY reduce the potential for violent conflicts with communities or workers, contribute to peace and stability in the regions where it operates, and demonstrate respect for the human rights of stakeholders affected by their operations.

This chapter draws on the Voluntary Principles on Security and Human Rights ("Voluntary Principles"), which provides a widely recognized framework for risk assessment and management of security providers that is respectful of human rights.[1] Entities are encouraged to become corporate participants in the Voluntary Principles initiative, to learn from and share knowledge with other companies and participants regarding best practices related to security and human rights.[2]

The International Code of Conduct for Private Security Providers and the recently published DCAF-ICRC Security and Human Rights Toolkit provide additional content, guidance and recommendations, that are highly relevant to mining and mineral processing activities.

KEY REFERENCES

This chapter strongly builds on, or aligns with, the following international or multilateral frameworks, conventions, and guidance:

- The International Bill of Human Rights (including the 1966 International Covenant on Civil and Political Rights (ICESCR) and International Covenant on Economic, Social and Cultural Rights (ICCPR))
- United Nations Guiding Principles for Business and Human Rights, 2011
- The Voluntary Principles on Security and Human Rights, 2000 (latest version 2023)
- The Voluntary Principles on Security and Human Rights Implementation Guidance Tools, 2021
- ICoCA International Code of Conduct for Private Security Providers, 2010
- DCAF-ICRC Security and Human Rights Toolkit, 2023
- UN Basic Principles on the Use of Force and Firearms by Law Enforcement Official, 1990
- UN Code of Conduct for Law Enforcement Officials, 1979
- IFC Performance Standard 4: Community Health, Safety, and Security, 2012

OBJECTIVE OF THIS CHAPTER

To manage private and public security in a manner that protects workers, communities, operations, assets, and products without infringing on human rights.

SCOPE OF APPLICATION

This chapter is applicable to all exploration, mining and mineral processing projects and operations. For each requirement, the following colors are displayed in the margin to indicate the phases for which it is required:

E1	Exploration – Stage 1
E2	Exploration – Stage 2
E3	Exploration – Stage 3
D	Project Development and Permitting
M	Operating Mine
P	Operating Mineral Processor

CRITICAL REQUIREMENTS IN THIS CHAPTER

Throughout the Standard, critical requirements are identified using a red frame.
There are two (2) **critical requirements** in this Chapter.

OPTIONAL IRMA+ REQUIREMENTS IN THIS CHAPTER

Throughout the Standard, optional IRMA+ requirements are identified using a dotted blue frame. There is one (1) **optional IRMA+ requirement** in this Chapter.

In this second draft, IRMA introduces a new category of requirements: IRMA+. These requirements are aspirational and forward-looking. They reflect emerging expectations and recommendations from stakeholders, but currently go above and beyond existing and established best practice. IRMA+ requirements are entirely optional, and they will not affect the scores and achievement levels obtained by the entities choosing to be assessed against them.

IRMA Requirements

3.4.1 Formalized Policy

E2 E3 D M P

3.4.1.1 The ENTITY has a formal policy in place that:

a. Commits to integrate the respect of all internationally recognized human rights[3] in its efforts to maintain the security of the site, associated facilities and transport routes[4];

b. Commits to avoid hiring security personnel and using private or public security forces that have been credibly implicated in the infringement of human rights, breaches of international humanitarian law or the excessive use of force[5];

c. Sets clear expectations for how employees, contractors, and other relevant parties[6] linked to the site and its associated facilities shall respect these commitments (a. and b.); and

d. Is approved at the top management level of the ENTITY;

e. Is proactively communicated to employees, contractors, and other relevant parties[7] linked to the site and its associated facilities;

f. Is publicly accessible; and

g. The ENTITY has allocated financial and staffing resources to implement this policy at the level of the site.

3.4.2 Risk and Impact Assessment

E2 E3 D M P

3.4.2.1 A risk and impact assessment (or equivalent) is carried out and documented by competent professionals to identify and assess potential adverse human rights, social, or safety impacts (hereafter referred to as 'risks') and actual adverse impacts that may arise from the site's security context and the ENTITY's security management and arrangements, as follows:

a. This assessment follows a credible methodology, and the methodology used is documented[8];

b. This assessment includes an analysis of the political and security context in the country of operation[9];

c. It is informed by credible information obtained from a range of perspectives, including affected rights-holders and stakeholders, as well as other relevant stakeholders such as Rights Defenders, and expert advice[10];

d. It assesses risks and impacts associated with the site's security context and the ENTITY's management and use of private security personnel and the use or deployment of public security forces[11] (hereafter referred to collectively as 'security-related risks and impacts' on affected people and communities[12], including differential risks and impacts on different categories of stakeholders and rights-holders[13];

e. It assesses security-related risks and impacts on workers and visitors, including differential risks and impacts of different categories of workers[14]; and

f. It assesses security-related risks and impacts on the site and its associated facilities[15].

E2 E3 D M P

3.4.2.2 If the suspected or confirmed presence of conflicts or high risks in the site's area of influence has been identified as per Chapter 1.3, the risk and impact assessment integrates the findings and recommendations of the Heightened Risk and Impact Assessment required in Chapter 1.5.

3.4.3 Management Plan and Procedures

E2 E3 D M P

3.4.3.1 Building on 3.4.2 and other relevant sources of information[16], a security management plan (or equivalent) is developed and documented by competent professionals, to prevent, mitigate and remedy all identified risks and impacts related to the site's security context and the ENTITY's management and use of private security personnel and public security forces, as follows:

a. This plan outlines specific measures, that strictly align with the mitigation hierarchy, to prevent and, where prevention is not possible or not immediately possible, to mitigate and remedy all the potential risks and actual adverse impacts identified;

b. Where it is necessary to prioritize measures to address actual and potential adverse impacts, it first seeks to prevent and mitigate those that are most severe or where delayed response would make them irremediable[17];

c. It includes qualitative and quantitative performance indicators (including gender-disaggregated indicators and other categories of disaggregated indicators where appropriate),[18] linked to adequate baseline data, to enable monitoring and evaluation of the effectiveness of measures over time;

d. It assigns implementation of measures to responsible staff with adequate skills and expertise;

e. It assigns responsibility to its top management level to oversee plan implementation, monitoring, and recordkeeping[19];

f. It includes clearly-defined timelines and an implementation schedule that specifies the expected outcomes for affected rights-holders and stakeholders;

g. It maintains estimates of human resources and budget required; and

h. It includes a financing plan in place to ensure that funding is available for the effective implementation of the plan.

E2 E3 D M P

3.4.3.2 If the risk and impact assessment required in 3.4.2, or any other credible information, reveals the potential for conflicts, or actual conflicts between the ENTITY's private security personnel and affected communities or workers, the security management plan also includes:

a. Specific mitigation strategies to address potential and/or actual conflicts, developed in collaboration with communities and/or workers;

b. Inclusive collaboration with communities and/or workers to take into consideration the needs of different genders, ages, and ethnicities, and any potentially underserved and/or marginalized people, in accordance with Chapter 1.2; and[20]

c. If specific risks or impacts to human rights are identified in the assessment, mitigation strategies conform with the relevant requirements of Chapter 1.3[21].

E2 E3 D M P

3.4.3.3 Critical Requirement

The ENTITY has procedures in place regarding the use of force and firearms that require that the private security personnel used/deployed for the security of the site, associated facilities, and transport routes[22]:

a. Take all reasonable steps to exercise restraint and utilize non-violent means before resorting to the use of force;

b. If force is used, it does not exceed what is strictly necessary, it is proportionate to the threat and appropriate to the situation, and it is systematically investigated and reported; and

c. Are unarmed unless the risk analysis prescribes such a need, and firearms are only used for the purpose of self-defense or the defense of others if there is an imminent threat of death or serious injury.

E2 E3 D M P

3.4.3.4 Affected rights-holders and stakeholders, including Rights Defenders and civil society organizations, have access to a grievance mechanism to raise, and seek resolution or remedy for, complaints and grievances specifically related to the ENTITY's security management and arrangements, as follows:

a. A grievance mechanism through which affected rights-holders and stakeholders, including Rights Defenders and civil society organizations, can raise, and seek resolution or remedy for, complaints and grievances specifically related to the ENTITY's security management and arrangements, is in place[23];

b. This grievance mechanism is rights-compatible[24];

c. Affected rights-holders and stakeholders have been informed about the existence and functioning of this grievance mechanism, as well as of other relevant mechanisms[25];

d. If the operational-level grievance mechanism developed as per Chapter 1.6 (Complaints and Grievance Mechanism and Access to Remedy) is used as the mechanism to receive complaints and grievance specifically related to the ENTITY's security management and arrangements, the Entity fully meets all requirements in Chapter 1.6; and

e. If a separate mechanism is created to handle only complaints and grievances related to human rights, it is established and managed in a manner that fully meets all requirements in Chapter 1.6.

3.4.4 Selection and Vetting of Security Personnel

E2 E3 D M P

3.4.4.1 The ENTITY has a system in place for the selection and vetting of **private security personnel**[26], to ensure that the ENTITY:

a. Develops a selection protocol (for employees) that lays out clear terms on exclusion criteria[27], and develops a request for proposals (for private security providers) that lays out clear terms on exclusion criteria[28], award criteria, needed personnel and required weapons and equipment, and that requires each applicant to provide background information;

b. Evaluates applications and bids according to the requirements laid out in the selection protocol or request for proposals, and conducts comprehensive due diligence[29] on the selected individuals and provider/s; and

c. Ensure the selected private security providers have effective vetting programs in place too, and encourages them to sign a formal declaration that none of their employees have been implicated in abuses of human rights and/or violations of international humanitarian law and/or the use of excessive force.

E2 E3 D M P

3.4.4.2 The ENTITY has a system in place for the vetting of **public security forces** used/deployed to provide security to the site, associated facilities and/or transport routes to ensure that the ENTITY, to the extent possible[30]:

a. Maintains communication and working relationships, commensurate with the level risks and impacts associated with public security forces, with different echelons of public security forces and actively seek opportunities to discuss vetting procedures;

b. In collaboration with the relevant government authorities, identifies which institutions should be consulted in order to conduct background checks;

c. Uses multiple sources to obtain relevant information[31]; and

d. Establishes procedures to help ensure that individuals who have been convicted of, or credibly implicated in, the infringement of human rights, breaches of international humanitarian law, or the use of excessive force, do not provide security services for the ENTITY.

3.4.5 Arrangements with Private and Public Security Forces

E2 E3 D M P

3.4.5.1 If **private security** is used to provide security to the site, associated facilities, and/or transport routes, the ENTITY has signed contract/s with each private security provider that:

a. Sets out the following agreed-on principles: 1) Private security must act consistently with the law and international guidelines; 2) Private security must respect the Entity's procedures regarding the use of force and firearms required in 3.4.3.3; 3) Allegations of human rights abuses will be investigated and monitored; 4) Only preventative and defensive services are to be provided; 5) Individuals implicated in human rights abuses are not permitted to provide security services to the Entity; and 6) Private security must investigate and report to the ENTITY incidents where physical force is used;

b. Delineates respective duties and obligations with respect to the provision of security in and around the site and associated facilities and, if relevant, along transport routes, and with respect to the reporting of any security-related incidents;

c. Requires the private security provider to ensure its personnel are trained to respect the rights of the workers and local community members, and outlines the content and frequency or the required training;

d. Stipulates how the ENTITY monitors the conduct of **private security** personnel and holds them accountable;

e. Stipulates termination of relationship between the ENTITY and the **private security** provider where there is credible evidence of unlawful or abusive behavior by the latter; and

f. Stipulates how the ENTITY engages with national judicial authorities for crimes or human rights violations by **private security** personnel.

E2 E3 D M P

3.4.5.2 If **public security forces** are used/deployed to provide security to the site, associated facilities, and/or transport routes, the ENTITY makes a good faith effort to sign a Memorandum of Understanding or similar agreement[32] with each public security provider/agency that includes similar provisions to those in 3.4.5.1.

3.4.6 Training of Security Personnel

E2 E3 D M P

3.4.6.1 The entity ensures that initial training prior to deployment, and refresher courses:

a. Are mandatory for all private security personnel[33];

b. Include information related to ethical conduct, and respect for the rights of workers, Indigenous rights-holders (if applicable), and affected communities, with specific reference to groups and individuals disproportionately affected by human rights violations[34];

c. Include first-aid provision, conflict management and dealing with incidents and disturbances[35]; and

d. Include the ENTITY's procedures on the appropriate use of force and firearms required in 3.4.3.3.

E2 E3 D M P

3.4.6.2 If **public security forces** have been, or are to be, used/deployed to provide security to the site, associated facilities, and/or transport routes, the ENTITY has a system to:

a. Determine whether public security personnel are provided with effective training on, and have accurate understanding of, all the topics listed in 3.4.6.1;

b. Where gaps in training and/or understanding are identified, the ENTITY offers to facilitate[36] initial training and refresher courses for public security personnel that are (or will be) used/deployed to provide security to the site, associated facilities, and/or transport routes; and

c. Support any existing relevant training programs, and any current or potential future technical assistance programs being offered by donors/home country governments[37] if applicable.

3.4.7 Response to Security Incidents

E2 E3 D M P

3.4.7.1 **Critical Requirement**

The ENTITY has a system in place to investigate and respond to security incidents, as follows:

a. Investigation of, and response to, security incidents occur in accordance with all relevant terms of the security arrangements required in 3.4.5;

b. The ENTITY documents and investigates all use of force and security incidents, including those involving impacts on human rights or the inappropriate use of force[38];

c. The ENTITY takes appropriate measures to prevent[39], and where prevention is not possible or not immediately possible, mitigate and provide remediation for human rights impacts (as per Chapter 1.3),[40] injuries, or fatalities caused by private security personnel and/or public security forces (in accordance with Section 3.4.3); and

d. The ENTITY takes appropriate measures, including disciplinary measures, to prevent and deter abusive or unlawful acts by security personnel, and acts that contravene the ENTITY's security arrangements and procedures on the use of force and firearms and/or its human rights policies and other relevant policies.

E2 E3 D M P

3.4.7.2 If an actual security incident occurs (or has occurred), the ENTITY:

a. Documents and investigate the incident, and take the appropriate measures required in 3.4.7.1;

b. Provides medical assistance to all injured people, including offenders, and ensures the safety of victims and those filing security-related allegations;

c. Reports the incident, including any credible allegations of human rights abuses by private or public security providers, to competent authorities and national human rights institutions; and

d. Cooperates in any investigations or proceedings led by relevant authorities or human rights institutions.

E2 E3 D M P

3.4.7.3 Besides the measures required in 3.4.7.2 for all security incidents, in the event of security-related incidents that result in injuries, fatalities, or alleged human rights impacts, the ENTITY:

a. Provides the people affected[41] with information on the incidents and on any investigations that are underway;

b. Collaborates with the people affected, and their advisors if applicable, to develop and agree on qualitative and quantitative indicators to track the effectiveness of responses; and

c. Collaborates with the people affected, and their advisors if applicable, to conduct lessons-learned exercises, and develop and implement strategies to prevent the recurrence of similar incidents.

E2 E3 D M P

3.4.7.4 **IRMA+**

Besides the collaboration required in 3.4.7.3.c, the ENTITY seeks to collaborate with other relevant stakeholders including civil society, human rights experts, security providers, representatives of the country of operation's government, and other companies to share lessons learned and address challenges in the management of security risks and impacts.

3.4.8 Meaningful Engagement with Stakeholders

E2 E3 D M P

3.4.8.1 The ENTITY engages with affected rights-holders and stakeholders on security issues as follows:

a. Engagement occur in a manner that is inclusive of different genders, ages, and ethnicities and any potentially underserved and/or marginalized people;

b. Stakeholders, including country of operation's government/authorities and affected rights-holders and stakeholders, are consulted about the impact of the ENTITY's security management and arrangements on those stakeholders;

c. The consultations occur at a frequency commensurate with the risks associated with the site's security context and the ENTITY's security management and arrangements, as identified per 3.4.2 and updated per 3.4.10[42]; and

d. The policy required in 3.4.1 is proactively shared with relevant stakeholders[43]; and

e. Affected rights-holders and stakeholders are regularly offered a briefing on the ENTITY's procedures on the use of force and firearms required in 3.4.3.3.

3.4.9 Monitoring and Evaluation

E2 E3 D M P

3.4.9.1 To monitor and evaluate the effectiveness and appropriateness of its security management and arrangements, at least annually, the ENTITY:

a. Tracks and documents its performance, over successive time periods, against the indicators defined in 3.4.3.1 in 3.4.7.3;

b. Tracks and documents how the measures developed and implemented as per 3.4.3, 3.4.4, 3.4.5, 3.4.6, and 3.4.7 are effectively preventing actual security incidents and adverse impacts, and where prevention was not possible or immediately possible, providing timely and adequate remediation to victims and affected people; and

c. Disaggregates the data according to gender-indicators where appropriate.

E2 E3 D M P

3.4.9.2 The monitoring and evaluation process:

a. Encourages and facilitates joint tracking or joint fact-finding with affected communities and workers, in a manner that is inclusive of different genders, ages, and ethnicities, and any potentially underserved and/or marginalized people, as per Chapter 1.2[44];

b. Includes continuous feedback from internal and external sources, including from joint tracking and joint fact-finding with affected communities and workers; and

c. Includes safeguards to protect the security and privacy of collected personal data or characteristics of people[45].

3.4.10 Continuous Improvement

E2 E3 D M P

3.4.10.1 At least annually, but without undue delay after a significant change, the ENTITY:

a. Reviews the monitoring and evaluation results, informed by internal and external feedback, as per Section 3.4.9;

b. Reviews any security-related grievances and the functioning of the relevant grievance mechanism/s required in 3.4.3.4 (see also Section 1.6.4);

c. Reviews its effectiveness in preventing, responding to, and remediating, actual security incidents, including those involving impacts on human rights or the inappropriate use of force, informed by the monitoring and evaluation required in 3.4.9.1 and 3.4.9.2;

d. Develops and implements time-bound corrective measures to update, if necessary[46], the risk and impact assessment in accordance with Section 3.4.2;

e. Develops and implements time-bound corrective measures to update, if necessary[47], the security management plan and procedures in accordance with Sections 3.4.3 to 3.4.8; and

f. Develops and implements time-bound corrective measures to update, if necessary[48], its monitoring and evaluation processes in accordance with Section 3.4.9.

3.4.11 Information-Sharing and Public Reporting

E2 E3 D M P

3.4.11.1 At least annually, and with due regard for rights-holders safety, data privacy, and for security concerns, the ENTITY makes publicly accessible updated versions of, and maintains[49] publicly accessible all previous versions of[50]:

a. Key findings of the monitoring and evaluation process required in 3.4.9, and of the review process required in 3.4.10.1;

b. A summary of the measures developed and implemented as per 3.4.3, 3.4.4, 3.4.5, 3.4.6, and 3.4.7, and the extent to which they effectively prevented actual security incidents and adverse impacts, and where prevention was not possible or immediately possible, provided timely and adequate remediation to victims and affected people; and

c. A list of the time-bound corrective measures identified as per 3.4.10.1.

E2 E3 D M P

3.4.11.2 If public security forces are providing security for any aspect of the operation, the ENTITY encourages the country of operation's government/authorities to make (or allow the ENTITY to make) details[51] about their security arrangements transparent and accessible to the public, subject to any overriding safety and security concerns[52].

CROSS REFERENCES TO OTHER CHAPTERS

This table will be added when the new content for all chapters is finalized and approved.

CHAPTER ENDNOTES

[1] Voluntary Principles on Security and Human Rights. 2014. www.voluntaryprinciples.org

[2] ibid. "Voluntary Principles Initiative – Guidance on Certain Roles and Responsibilities of Companies." https://www.voluntaryprinciples.org/wp-content/uploads/2019/12/RolesResponsibilities-Companies.pdf

[3] Including not violating the rights of individuals while exercising their right to freedom of association or their right to strike.

[4] See also Chapter 1.3.

[5] These commitments may be made in a broader Human Rights Policy (see Chapter 1.3), or another relevant policy.

[6] This may include, as relevant, joint venture partners' staff and contractors responsible for operation/management, organizations or public agencies visiting the site, as well as country of operations' government and authorities responsible for the use/deployment of public security forces, if applicable.

[7] This may include, as relevant, joint venture partners' staff and contractors responsible for operation/management, organizations or public agencies visiting the site.

[8] Risk assessments typically include: establishment of scope; identification of sources of risk; identification of risks; assessment of risks; development of risk treatment and mitigation measures; and communications, monitoring and assessment, and revision. The assessment of security risks may be integrated in existing risk assessment processes.

[9] E.g., the human rights records of the government and specific public and private security forces, adherence to the rule of law, potential for corruption, national labour laws, private security regulation, and track record and ESG performance of local private security providers.

[10] Special effort should be made to include women, children or their representatives, and other groups who may be particularly vulnerable to impacts from security arrangements (e.g., this might include artisanal and small-scale miners, human rights defenders, or youth). Other relevant local stakeholders may include local government or community leaders, civil society organizations or other companies operating in the area. Expert advice may come from governments, multi-stakeholder initiatives, human rights institutions, civil society, or academics with local knowledge and expertise.

[11] Including the risks related to the presence and equipping of security forces (e.g., risks associated with equipment transfers such as misappropriation or diversion of security equipment; and increased risk of the use of force or violence associated with firearms or other equipment).

[12] E.g., conflict risks between security forces and communities during social protest, etc.

[13] Considering gender, age, ethnicity, disability, potentially underserved and/or marginalized people, or any other factor of factor of disproportionate exposure or susceptibility to risks/impacts in the project's/operation's area of influence (such as Rights Defenders and Indigenous rights-holders). See also Chapter 2.3 and requirements for an Intersectional Gender Impact Assessment.

[14] Especially women workers, and LGBTIQA+ workers. See also Chapter 2.3 and requirements for an Intersectional Gender Impact Assessment.

[15] E.g., protecting assets and goods from being vandalized or stolen.

[16] Other sources of information may include data from monitoring and evaluation, discussions with or grievances filed by stakeholders or workers, internal reviews of particular issues that relate to the security context and/or human rights, etc.

[17] Once the most severe and most likely adverse impacts are addressed within a reasonable time, the ENTITY will address less severe and less likely adverse impacts.

[18] Other disaggregation may be by age, ethnicity, disability, vulnerability status, proximity to the operation, etc.

[19] If work is carried out by third party contractors, then there needs to be a staff employee responsible for overseeing the quality of work, timelines, etc.

[20] Which stakeholders must be included and what may constitute 'underserved and/or marginalized people' requiring additional focus depends on the context. Entities should draw on stakeholder mapping, stakeholder interviews, project documentation, as well as site observations to determine whether all relevant stakeholders have been identified and included. For this requirement, particular attention should be paid to those with existing forms of vulnerability to security-related incidents such as women, girls, those located close to risk factors such as workers' camps or major transportation routes.

[21] IRMA Standard, Chapter 1.3—Human Rights Due Diligence. See specifically Section1.3.4.

[22] The requirements in this Section align with provisions 30 and 31 of the ICoCA Code of Conduct for Private Security Providers. Available at: https://icoca.ch/the-code/

[23] The operational-level grievance mechanism developed as per IRMA Chapter 1.6 (Complaints and Grievance Mechanism and Access to Remedy) may be used as the mechanism to receive all types of complaints, including those related to the ENTITY's security management and arrangements, or a separate mechanism may be created to handle only those complaints and grievances. If a separate mechanism is developed, it shall be done in a manner that is consistent with Chapter 1.6 (see subrequirements d. and e.). Also, there may be other mechanisms that are not operated by the company through which stakeholders or rights-holders can seek

recourse (e.g., administrative, judicial and non-judicial remedies), and these options should be mentioned to stakeholders who file security-related grievances with the company.

[24] 'Rights-compatible' means ensuring that outcomes and remedies accord with internationally-recognized human rights.

[25] There may be other mechanisms that are not operated by the ENTITY through which stakeholders or rights-holders can seek recourse (e.g., administrative, judicial and non-judicial remedies), and these options should be mentioned to stakeholders who file grievances with the company.

[26] Hired as employees and contracted through private security providers. These expectations are aligned with the Voluntary Principles on Security and Human Rights, and the DCAF-ICRC Security and Human Rights Toolkit,

[27] This should include exclusion of individuals who have been convicted of, or credibly implicated in, the infringement of human rights, breaches of international humanitarian law or the use of excessive force.

[28] This should include exclusion of businesses and individuals who have been convicted of, or credibly implicated in, the infringement of human rights, breaches of international humanitarian law or the use of excessive force.

[29] Whether conducted internally or by a third party outfit, companies should investigate the following factors during the private security due diligence process: – History of respect for/violations of human rights law and international humanitarian law – Personal and business reputation – Management style and ethics of key executives – Litigation and criminal offence history – Training provided by the company to its employees on human rights and humanitarian law – Business licenses – Equipment licenses (particularly as these relate to weapons and firearms) – Procedures on use of force and firearms (see Annex H) – Undisclosed or misrepresented assets, losses, and projections – Operational history – Compliance with labour, health, safety and environmental regulations – Conflicts of interest – Corporate culture – Other liabilities and risks (VP Implementation Guidance Tool. pp. 52, 53).

[30] These expectations are aligned with the Voluntary Principles on Security and Human Rights, and the DCAF-ICRC Security and Human Rights Toolkit,

[31] Sources include: When legally authorized, check police records for any criminal records or warrants; public security personnel records, if it is legal and possible to do so; investigate the historical conduct of public security forces in the region, focusing on any allegations of misconduct or abuse; In some countries, security companies that specialize in political risk advice, investigations and security consultancy are capable of and legally allowed to conduct thorough background investigations that are beyond the scope of those conducted by a company security department. For other possible sources see: DCAF-ICRC Security and Human Rights Toolkit, pp. 73 and 74.

[32] If it is not possible to agree on a full MoU, the ENTITY may develop specific agreements with public security providers and/or the country of operation's government/authorities around key areas of concern such as training, equipment transfers or the working relationship between the ENTITY and public security forces.

[33] Whether employees of the ENTITY or contractors.

[34] Training content should cover: international humanitarian law (IHL), gender-related topics including prevention of sexual abuse and sexual- and gender-based violence, exploitation and harassment, anti-bribery and anti-corruption measures, and respect for the local population and culture, including Indigenous Peoples.

[35] E.g. public disorder, lawful and unlawful protests, strikes, labour disputes and evictions, ensuring these duties and responsibilities do not conflict with the mandate of public security forces.

[36] Facilitating may include partnering with other stakeholders and organizations, and content and regularity of the training is agreed with the relevant authorities.

[37] E.g. cooperation on security sector reform

[38] As required in critical requirement 3.4.3.3.

[39] Prevention may be achieved through early alert system and pro-active monitoring.

[40] IRMA Standard, Chapter 1.3—Human Rights Due Diligence. (See specifically Section 1.3.4).

[41] Which could be community members and/or workers.

[42] Depending on the circumstances, there may not be a need for regular consultations (e.g., the commodity being mined is not high value so the level of security at the site is low, security guards are not armed, and there is no nearby community), whereas in situation where there are more obvious risks to communities from security arrangements frequent consultation may be necessary (e.g. fragile human rights situation, whether the ENTITY operates in a conflict-affected or high-risk area, as well as possible link to international humanitarian law (IHL) violation).

[43] Relevant stakeholders could include women, children or their representatives, and other groups who may be particularly/disproportionately affected by adverse impacts from, and infringements of human rights by, security arrangements (e.g., this might include ASM operators, rights defenders, and youth). Other relevant local stakeholders may include local government or community leaders; civil society organizations; and other companies operating in the area.

[44] This is especially relevant for contexts where your business and (potentially) affected rights-holders are in dispute about a particular (potential) adverse impact, and rights-holders are unlikely to accept the business' own tracking of the effectiveness of its response to it.

[45] Especially of people at heightened risk of vulnerability and marginalization, including children, or any other sensitive data.

[46] This will be informed by the monitoring and evaluation process required in the previous Section, and on the review process required in a. to c. Including if there have been changes to the operation (e.g., expansions, changes in practices, etc.) or operating environment that have created new risks that need to be mitigated, or exacerbated existing ones.

[47] This will be informed by the monitoring and evaluation process required in the previous Section, and on the review process required in a. to c.

[48] This will be informed by the monitoring and evaluation process required in the previous Section, and on the review process required in a. to c.

[49] All material must remain publicly accessible at least until the completion of all post-closure activities (including any previous versions, iterations and revisions). Note that the intention is not that the reports should be removed from the public domain after that. Rather, where possible, it should be retained indefinitely as the information may be important for legal or other purposes.

[50] This reporting could be part of the reporting on human rights due diligence required in Chapter 1.3.

[51] Such as the purpose and nature of the actions taken by public security forces in relation to the site, its associated facilites, and/or transportation routes.

[52] As explained in the Voluntary Principles Implementation Guidance Tool, information that could create security and safety concerns or human rights risks would include specific troop movements, supply schedules, company personnel movements, locations of valuable or hazardous equipment, etc.). ICMM, IFC and IPIECA. 2012. Voluntary Principles on Security and Human Rights Implementation Guidance Tools. p. 47. https://www.voluntaryprinciples.org/wp-content/uploads/2021/11/Implementation-Guidance-Tools_English.pdf

www.responsiblemining.net

IRMA Initiative for Responsible Mining Assurance