

GRI 410: Security Practices 2016

410

EFFECTIVE DATE: 1 JULY 2018

TOPIC STANDARD

GRI 410: Security Practices 2016

Topic Standard

Effective Date

This Standard is effective for reports or other materials published on or after 1 July 2018

Responsibility

This Standard is issued by the [Global Sustainability Standards Board \(GSSB\)](#). Any feedback on the GRI Standards can be submitted to gssbsecretariat@globalreporting.org for the consideration of the GSSB.

Due Process

This Standard was developed in the public interest and in accordance with the requirements of the GSSB Due Process Protocol. It has been developed using multi-stakeholder expertise, and with regard to authoritative intergovernmental instruments and widely held expectations of organizations relating to social, environmental, and economic responsibilities.

Legal Liability

This document, designed to promote sustainability reporting, has been developed by the Global Sustainability Standards Board (GSSB) through a unique multi-stakeholder consultative process involving representatives from organizations and report information users from around the world. While the GRI Supervisory Board, Management Board, and GSSB encourage the use of the GRI Sustainability Reporting Standards (GRI Standards) and related Interpretations by all organizations, the preparation and publication of reports based fully or partially on the GRI Standards and related Interpretations are the full responsibility of those producing them. Neither the GRI Supervisory Board, Management Board, GSSB, nor Stichting Global Reporting Initiative (GRI) can assume responsibility for any consequences or damages resulting directly or indirectly from the use of the GRI Standards and related Interpretations in the preparation of reports, or the use of reports based on the GRI Standards and related Interpretations.

Copyright and trademark notice

This document is copyright-protected by Stichting Global Reporting Initiative (GRI). The reproduction and distribution of this document for information and/or use in preparing a sustainability report is permitted without prior permission from GRI. However, neither this document nor any extract from it may be reproduced, stored, translated, or transferred in any form or by any means (electronic, mechanical, photocopied, recorded, or otherwise) for any other purpose without prior written permission from GRI.

Global Reporting Initiative, GRI and logo, GSSB and logo, and GRI Sustainability Reporting Standards (GRI Standards) and logo are trademarks of Stichting Global Reporting Initiative.

© 2025 GRI. All rights reserved.

ISBN 978-90-8866-121-1

Content

Introduction	4
1. Topic management disclosures	7
2. Topic disclosures	8
Disclosure 410-1 Security personnel trained in human rights policies or procedures	8
Glossary	9
Bibliography	10

Introduction

GRI 410: Security Practices 2016 contains disclosures for organizations to report information about their security practice-related impacts, and how they manage these impacts.

The Standard is structured as follows:

- [Section 1](#) contains a requirement, which provides information about how the organization manages its security practice-related impacts.
- [Section 2](#) contains one disclosure, which provides information about the organization's security practice-related impacts.
- The [Glossary](#) contains defined terms with a specific meaning when used in the GRI Standards. The terms are underlined in the text of the GRI Standards and linked to the definitions.
- The [Bibliography](#) lists references used in developing this Standard.

The rest of the Introduction section provides a background on the topic, an overview of the system of GRI Standards and further information on using this Standard.

Background on the topic

This Standard addresses the topic of security practices. It focuses on the conduct of security personnel towards third parties, and the potential risk for excessive use of force or other violations of human rights. Security personnel can refer to employees of the reporting organization or employees of third-party organizations that provide security forces.

The use of security personnel can have negative impacts on local populations, and on the upholding of human rights and the rule of law. Providing effective training in human rights therefore helps to make sure that security personnel understand when to use force in an appropriate way, and how to ensure respect for human rights.

System of GRI Standards

This Standard is part of the GRI Sustainability Reporting Standards (GRI Standards). The GRI Standards enable an organization to report information about its most significant impacts on the economy, environment, and people, including impacts on their human rights, and how it manages these impacts.

The GRI Standards are structured as a system of interrelated standards that are organized into three series: GRI Universal Standards, GRI Sector Standards, and GRI Topic Standards (see [Figure 1](#) in this Standard).

Universal Standards: GRI 1, GRI 2 and GRI 3

[GRI 1: Foundation 2021](#) specifies the requirements that the organization must comply with to report in accordance with the GRI Standards. The organization begins using the GRI Standards by consulting *GRI 1*.

[GRI 2: General Disclosures 2021](#) contains disclosures that the organization uses to provide information about its reporting practices and other organizational details, such as its activities, governance, and policies.

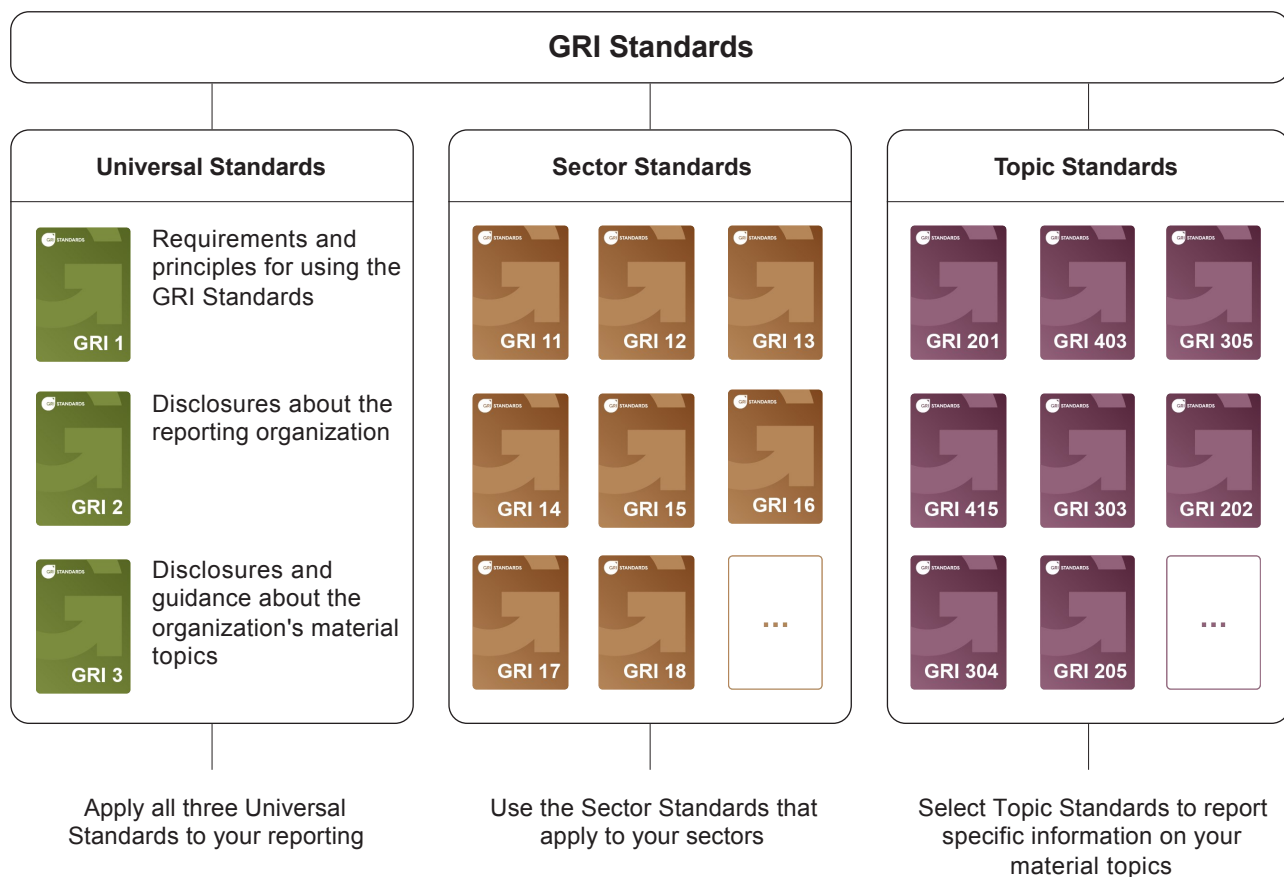
[GRI 3: Material Topics 2021](#) provides guidance on how to determine material topics. It also contains disclosures that the organization uses to report information about its process of determining material topics, its list of material topics, and how it manages each topic.

Sector Standards

The Sector Standards provide information for organizations about their likely material topics. The organization uses the Sector Standards that apply to its sectors when determining its material topics and when determining what to report for each material topic.

Topic Standards

The Topic Standards contain disclosures that the organization uses to report information about its impacts in relation to particular topics. The organization uses the Topic Standards according to the list of material topics it has determined using *GRI 3*.

Figure 1. GRI Standards: Universal, Sector and Topic Standards

Using this Standard

This Standard can be used by any organization – regardless of size, type, sector, geographic location, or reporting experience – to report information about its security practice-related impacts.

An organization reporting in accordance with the GRI Standards is required to report the following disclosures if it has determined security practices to be a material topic:

- [Disclosure 3-3 in GRI 3: Material Topics 2021](#) (see clause 1.1 in this Standard);
- Any disclosure from this Topic Standard that is relevant to the organization's security practice-related impacts (Disclosure 410-1).

See [Requirements 4 and 5 in GRI 1: Foundation 2021](#).

Reasons for omission are permitted for these disclosures.

If the organization cannot comply with a disclosure or with a requirement in a disclosure (e.g., because the required information is confidential or subject to legal prohibitions), the organization is required to specify the disclosure or the requirement it cannot comply with, and provide a reason for omission together with an explanation in the GRI content index. See [Requirement 6 in GRI 1: Foundation 2021](#) for more information on reasons for omission.

If the organization cannot report the required information about an item specified in a disclosure because the item (e.g., committee, policy, practice, process) does not exist, it can comply with the requirement by reporting this to be the case. The organization can explain the reasons for not having this item, or describe any plans to develop it. The disclosure does not require the organization to implement the item (e.g., developing a policy), but to report that the item does not exist.

If the organization intends to publish a standalone sustainability report, it does not need to repeat information that it has already reported publicly elsewhere, such as on web pages or in its annual report. In such a case, the organization can report a required disclosure by providing a reference in the GRI content index as to where this information can be found (e.g., by providing a link to the web page or citing the page in the annual report where the information has been published).

Requirements, guidance and defined terms

The following apply throughout this Standard:

Requirements are presented in **bold font** and indicated by the word 'shall'. An organization must comply with requirements to report in accordance with the GRI Standards.

Requirements may be accompanied by guidance.

Guidance includes background information, explanations, and examples to help the organization better understand the requirements. The organization is not required to comply with guidance.

The Standards may also include recommendations. These are cases where a particular course of action is encouraged but not required.

The word 'should' indicates a recommendation, and the word 'can' indicates a possibility or option.

Defined terms are underlined in the text of the GRI Standards and linked to their definitions in the [Glossary](#). The organization is required to apply the definitions in the Glossary.

1. Topic management disclosures

An organization reporting in accordance with the GRI Standards is required to report how it manages each of its material topics.

An organization that has determined security practices to be a material topic is required to report how it manages the topic using [Disclosure 3-3 in GRI 3: Material Topics 2021](#) (see clause 1.1 in this section).

This section is therefore designed to supplement – and not replace – Disclosure 3-3 in *GRI 3*.

REQUIREMENTS	1.1 The reporting organization shall report how it manages security practices using Disclosure 3-3 in GRI 3: Material Topics 2021.
--------------	--

2. Topic disclosures

Disclosure 410-1 Security personnel trained in human rights policies or procedures

REQUIREMENTS	<p>The reporting organization shall report the following information:</p> <ul style="list-style-type: none"> a. Percentage of <u>security personnel</u> who have received formal training in the organization's human rights policies or specific procedures and their application to security. b. Whether training requirements also apply to third-party organizations providing security personnel.
RECOMMENDATIONS	<p>2.1 When compiling the information specified in Disclosure 410-1-a, the reporting organization should:</p> <ul style="list-style-type: none"> 2.1.1 calculate the percentage using the total number of security personnel, whether they are <u>employees</u> of the organization or employees of third-party organizations; 2.1.2 state whether employees of third-party organizations are also included in the calculation.
GUIDANCE	<p>Guidance for Disclosure 410-1</p> <p>The training can refer either to training dedicated to the subject of human rights or to a human rights module within a general training program. Training can cover issues such as the use of force, inhuman or degrading treatment or discrimination, or identification and registering.</p> <p>Background</p> <p>The use of security personnel can play an essential role in allowing an organization to operate in a safe and productive manner, and can contribute to the security of local communities and populations.</p> <p>However, as set out in the International Code of Conduct for Private Security Service Providers, the use of security personnel can also have negative impacts on local populations and on the upholding of human rights and the rule of law.</p> <p>According to the UN Human Rights Office of the High Commissioner, 'human rights education constitutes an essential contribution to the long-term prevention of human rights abuses and represents an important investment in the endeavor to achieve a just society in which all human rights of all persons are valued and respected.'¹</p> <p>Training security personnel in human rights can therefore help to ensure their appropriate conduct towards third parties, particularly regarding the use of force. This disclosure indicates the proportion of the security force that can reasonably be assumed to be aware of an organization's expectations of human rights performance. Information provided under this disclosure can demonstrate the extent to which management systems pertaining to human rights are implemented.</p>

¹ United Nations Human Rights Office of the High Commissioner (OHCHR), <http://www.ohchr.org/EN/Issues/Education/Training/Pages/HREducationTrainingIndex.aspx>, accessed on 1 September 2016.

Glossary

This glossary provides definitions for terms used in this Standard. The organization is required to apply these definitions when using the GRI Standards.

The definitions included in this glossary may contain terms that are further defined in the complete [GRI Standards Glossary](#). All defined terms are underlined. If a term is not defined in this glossary or in the complete *GRI Standards Glossary*, definitions that are commonly used and understood apply.

E	employee individual who is in an employment relationship with the organization according to national law or practice
H	human rights rights inherent to all human beings, which include, at a minimum, the rights set out in the <i>United Nations (UN) International Bill of Human Rights</i> and the principles concerning fundamental rights set out in the <i>International Labour Organization (ILO) Declaration on Fundamental Principles and Rights at Work</i> Source: United Nations (UN), <i>Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework</i> , 2011; modified Note: See Guidance to 2-23-b-i in GRI 2: General Disclosures 2021 for more information on ‘human rights’.
I	impact effect the organization has or could have on the economy, environment, and people, including on their <u>human rights</u> , which in turn can indicate its contribution (negative or positive) to <u>sustainable development</u> Note 1: Impacts can be actual or potential, negative or positive, short-term or long-term, intended or unintended, and reversible or irreversible. Note 2: See section 2.1 in GRI 1: Foundation 2021 for more information on ‘impact’.
M	material topics topics that represent the organization’s most significant <u>impacts</u> on the economy, environment, and people, including impacts on their <u>human rights</u> Note: See section 2.2 in GRI 1: Foundation 2021 and section 1 in GRI 3: Material Topics 2021 for more information on ‘material topics’.
S	security personnel individuals employed for the purposes of guarding property of the organization; crowd control; loss prevention; and escorting persons, goods, and valuables sustainable development / sustainability development that meets the needs of the present without compromising the ability of future generations to meet their own needs Source: World Commission on Environment and Development, <i>Our Common Future</i> , 1987 Note: The terms ‘sustainability’ and ‘sustainable development’ are used interchangeably in the GRI Standards.

Bibliography

This section lists references used in developing this Standard.

References:

1. International Code of Conduct for Private Security Service Providers, 2010.
2. Voluntary Principles on Security and Human Rights, <http://voluntaryprinciples.org/>, accessed on 1 September 2016.



PO Box 10039
1001 EA Amsterdam
The Netherlands

www.globalreporting.org