



Model Safety Policy for Newsrooms

Guinea-Bissau



Funded by the
European Union



REPORTERES
SEM FRONTEIRAS



FONDATION
HIRONNELLE

Acknowledgement

This document was produced within the framework of the 18-month media support project titled: *“Promote and Protect Democracy by Safeguarding Freedom of Opinion and Expression and Combating Mis/Disinformation in Guinea-Bissau.”*

The project is funded by the European Union and implemented by the Media Foundation for West Africa (MFWA) in collaboration with Reporters Without Borders (RSF) and Fondation Hirondeille (FH).

Disclaimer

The contents of this document are the sole responsibility of the Media Foundation for West Africa (MFWA) and can under no circumstances be regarded as reflecting the position of the European Union.

Table of Contents

Introduction	—	1
1. Policy Statement	—	2
2. Integrated Safety	—	3
3. Scope	—	3
4. Roles and Responsibilities	—	4
5. Risk Assessment	—	5
6. Physical Safety	—	5
7. Digital Safety	—	5
8. Protection of Sources	—	6
9. Legal Protection	—	6
10. Editorial Safety	—	6
11. Psychosocial Support	—	7
12. Incident Response	—	7
13. Institutional Cooperation	—	8
14. Training	—	8
15. Review and Accountability	—	8
16. Operational Annexes	—	9
Annex A: Risk Assessment Checklist	—	10
Annex B: Emergency Contact Sheet	—	13
Annex C: Digital Security Guidelines	—	14
Annex C (2): Digital Security Checklist	—	15
Annex D: Security Incident Log	—	16
Annex E: Security Checklist for Sensitive Publications	—	18

Introduction

This Newsroom Safety Policy has been developed under the EU-funded project implemented by the Media Foundation for West Africa (MFWA) as Coordinator, in partnership with Reporters Without Borders (RSF) and Fondation Hironnelle (FH) and validated by the Media Groups and Associations in Guinea-Bissau. It was subsequently reviewed and finalised following a participatory validation process involving media organisations and media professionals from Guinea-Bissau.

The policy comes at a time when journalists and media professionals in the country face a wide range of risks, including threats, harassment, physical violence, digital attacks, legal intimidation, political pressure, editorial interference, and alarming levels of psychosocial stress.

The document is based on the UN Plan of Action on the Safety of Journalists (UNESCO/UN), UNESCO Safety Indicators, guidelines from RSF, CPJ, IFJ, IMS, and legal provisions enshrined in the Constitution of the Republic of Guinea-Bissau and the Press Law.

Its purpose is to establish an integrated safety model to protect media professionals, strengthen newsroom security and protect press freedom.

The policy's effectiveness depends on its continuous implementation, regular monitoring and effective integration into the day-to-day running of newsrooms.

1. Policy Statement

This Safety Policy is an integral part of the editorial team's institutional culture and is binding on all its members, employees and partners.

The newsroom is committed to:

- Prioritize human safety above editorial primacy or publication deadlines.
- Adopt a zero-tolerance stance against violence, harassment, intimidation, or threats.
- Implement specific measures to prevent and respond to harassment, intimidation and violence against female journalists and other vulnerable groups;
- Incorporate Integrated Safety (physical, digital, legal, editorial, psychosocial, and source protection) into all phases of journalism.
- Promote a culture of prevention, solidarity, and collective responsibility.
- Ensure that no journalist will suffer harm, sanctions, or retaliation for reporting on security/safety incidents.

2. Integrated Safety

Integrated Safety combines and articulates six essential dimensions:

1. Physical Safety
2. Digital Safety
3. Legal Safety
4. Psycho-social Safety
5. Editorial and Ethical Safety
6. Protection of Sources and Whistleblowers

These dimensions must be addressed in a coordinated manner, recognising that weaknesses in one area can undermine the overall safety of the newsroom.

3. Scope

This policy applies to:

- Full-time journalists, freelancers and collaborators
- Editors, management and support staff
- Interns and students gaining professional experience
- National or international assignments linked to newsroom duties

The editorial team recognises that freelancers, young journalists and interns may face increased vulnerabilities and should therefore benefit from adequate protection and support mechanisms.

4. Roles and Responsibilities

Role	Responsibility
<i>Management/ Editors-in-Chief</i>	Ensure resources are allocated; approve assignments; provide equipment; decide on evacuation; oversee protocols; ensure legal and medical support.
<i>Safety Focal Person</i>	Maintain updated safety procedures; coordinate emergencies; keep emergency contacts; conduct briefings; monitor risks.
<i>Journalists and Staff</i>	Comply with safety guidelines; report threats; protect sources; use physical and digital equipment correctly.

The Safety Focal Person should have direct access to senior management and be able to immediately implement emergency response procedures.

Assigning specific responsibilities does not exempt a newsroom from the collective responsibility for the safety of all its members.

5. Risk Assessment

- A risk assessment must be carried out before any assignment involving sensitive environment.
- Assignments classified as high risk require senior approval and enhanced safety measures.
- Female journalists, young reporters and freelancers will receive additional consideration due to specific vulnerabilities.
- Forms and authorisations must be stored digitally for at least 12 months after the assignment.

6. Physical Safety

- Visible professional identification when appropriate.
- Adequate protective equipment.
- Safe transportation and continuous communication (check-in).
- Specific protocols for coverage of demonstrations, political rallies, and police operations.
- Evacuation procedures for emergency situations.

7. Digital Safety

- Strong passwords and two-factor authentication.
- Mandatory encryption of sensitive devices and data.
- Use only secure networks (VPN on open networks).
- Regular training on cybersecurity.
- Guidelines for responding to digital harassment and cyberattacks.

8. Protection of Sources

The newsroom guarantees:

- Confidentiality.
- Secure communication channels.
- Enhanced protection in sensitive investigations.
- Secure data storage.
- Prohibition of unauthorised disclosure.

9. Legal Protection

- Immediate access to legal support.
- Information on journalists' rights.
- Procedures in the event of detention, seizure of equipment or prosecution.
- Editorial verification protocols to minimize exposure to defamation or misinformation lawsuits.

All measures described must comply with the Constitution of the Republic of Guinea-Bissau, the Press Law and international human rights standards ratified by the State.

10. Editorial Safety

- Editorial decisions must consider impacts on safety.
- Cases of external interference must be recorded.
- Forced self-censorship or undue editorial pressure is prohibited.
- There should be specific guidelines for sensitive coverage.

11. Psychosocial Support

- Provision of debriefing after high-risk assignments.
- Referrals for psychosocial support.
- Prevention of traumatic stress and burnout.
- Enforcement of anti-harassment and anti-bullying measures.

The editorial team is committed to promoting an inclusive, safe and supportive environment.

12. Incident Response

- A confidential mechanism for staff to report safety incidents without fear of retaliation.
- Maintenance of an incident logbook.
- Production of quarterly reports for internal analysis.
- Cooperation with protection entities.

All major incidents must be assessed within 24 hours, with protective measures put in place immediately where necessary.

The editorial team shall conduct regular reviews of reported incidents, with a view to identifying risk patterns, improving protocols and strengthening preventive measures.

13. Institutional Cooperation

In case of detention, assault, disappearance, serious threat or illegal seizure:

- Immediate reporting to the relevant authorities.
- Contacting lawyers and organisations for protection.
- Assessing the need for additional institutional support.
- Formal request for investigation.

14. Training

- Regular newsroom-wide training.
- Inclusion of freelancers and interns.
- Simulation exercises for high-risk situations.
- Regular updates on digital, legal and operational security.

15. Review and Accountability

- This policy shall be reviewed annually.
- Feedback from staff will be incorporated.
- Non-compliance with the safety procedures may result in disciplinary measures.
- The implementation of the policy should be monitored on a regular basis.

16. Operational Annexes

Annex	Description
A	Risk Assessment Checklist
B	Emergency Contact Sheet
C	Digital Security Guidelines
C (2)	Digital Security Checklist
D	Security Incident Log
E	Security Checklist for Sensitive Publications

Closing Remarks

The safety of journalists does not depend solely on the formal existence of policies and protocols. It is built through continuous practice, institutional accountability, professional solidarity and a collective commitment to press freedom.

Annex A: Risk Assessment Checklist

To be completed before high-risk assignments (elections, protests, investigations, conflict coverage, travel to remote areas, etc.)

1. Details of Assignment

Assignment Title: _____

Date & Location: _____

Assigned Journalist(s): _____

Editor/Supervisor: _____

2. Instructions for Scoring

- Each item checked (✓) = 1 point.
- Each item Not checked = 0 points.
- Add up the total score for each section and overall.

Final Scoring:

- **0–6 points = Low Risk** (assignment can proceed with standard precautions)
- **7–12 points = Medium Risk** (enhance security measures)
- **13+ points = High Risk** (assignment requires extra support/resources or must reconsidered)

3. Assessment

A) Context and Environment (0–4)

- ☐ Politically sensitive assignment
- ☐ Involves protests/unrest/violence
- ☐ Area has recent threats to media/press restrictions
- ☐ Hostile groups likely to be present

Subtotal: ___ /4

B) Physical Safety (0–4)

- ☐ Travel at night or remote areas required
- ☐ Transport not secure or unreliable
- ☐ Protective gear required but not available
- ☐ No evacuation plan identified

Subtotal: ___ /4

C) Digital & Information Security (0–4)

- ☐ Devices not encrypted/password-protected
- ☐ Sensitive data or source info at risk
- ☐ VPN unavailable or unsafe internet expected
- ☐ Plan to protect sources not in place

Subtotal: ___ /4

D) Legal and Political Risks (0–3)

- ☐ Risk of arrest/detention
- ☐ Relevant laws not reviewed
- ☐ Legal support contacts unavailable

Subtotal: ___/3

E) Health and Well-Being (0–3)

- ☐ Known health risks in location
- ☐ Lack of valid medical insurance
- ☐ Psychosocial support not arranged

Subtotal: ___/3

F) Communication & Emergency Plan (0–4)

- ☐ Safety Focal Person not assigned
- ☐ Check-in plan not agreed
- ☐ Emergency contacts not shared
- ☐ Evacuation route not identified

Subtotal: ___/4

Overall Score: ___/22

- ☐ Approved ☐ Approved subject to conditions
- ☐ Not approved

Editor/Supervisor Name: _____

Signature: _____ **Date:** _____

Annex B: Emergency Contact Sheet

(To be updated regularly by the Safety Focal Person of each newsroom)

I. National Security and Emergency Services (Guinea-Bissau)

- **General emergency:** 112
- **Public Order Police:** 117 | 1414 (MTN) | 1515 (Orange)
- **Judicial Police:** 121
- **Fire & Rescue Service:** 118 | 1212 (MTN) | 1313 (Orange)
- **National Ambulance Service:** 119
- **Health Line:** 1919 (MTN) | 2020 (Orange)

II. Legal Support

- **Liga Guineense dos Direitos Humanos (LIGA):**
+245 95 333 222 | liga.guinebissau@gmail.com
- **MFWA's West Africa Network of Activists and Media Defence Lawyers (WANAMDEL)**
+233 302 555 327 | +233 302 955 213 | info@mfwf.org

(Every newsroom is advised to include its own lawyers or additional local contacts)

Annex C: Digital Security Guidelines

1. Device and Account Security

- Use **strong, unique passwords** (≥12 characters).
- Activate **2FA** on email and social media.
- Regularly update devices.
- Lock laptops and phones.
- Do not share devices without proper security clearance.

2. Safe Communication

- Use Signal or WhatsApp for sensitive exchanges.
- Avoid public Wi-Fi without using a **VPN**.
- Back up critical data regularly.
- Always verify the identity of contacts.

3. Protecting Sources

- Encrypt sensitive data.
- Using pseudonyms for vulnerable sources.
- Avoid storing unnecessary data.
- Delete sensitive data when no longer needed.

4. Social Media

- Avoid sharing personal information.
- Separate professional and personal accounts.
- Do not engage in hostile online exchanges.
- Report online harassment immediately to the Safety Focal Person.

5. Digital Incident Response

- Immediately disconnect compromised devices from the internet.
- Document evidence (screenshots, emails, messages).
- Inform the Safety Focal Person and newsroom IT support.
- Report to trusted protection partners.

Annex C (2): Digital Security Checklist

1. Before Leaving for Assignment

- ☐ Devices fully charged and updated
- ☐ Strong passwords and 2FA enabled
- ☐ VPN installed and tested
- ☐ Encrypted apps ready
- ☐ Sensitive data encrypted
- ☐ Backup completed
- ☐ Sources' identities anonymized
- ☐ Social media checked
- ☐ Emergency contacts saved

2. During Assignment

- ☐ Avoid public Wi-Fi unless VPN is active
- ☐ Do not share devices
- ☐ Be cautious of suspicious links/attachments
- ☐ Maintain regular check-ins with the Safety Focal Person

3.If Incident Occurs

- ☐ Disconnect device from internet
- ☐ Take screenshots/evidence
- ☐ Report to Safety Focal Person
- ☐ Escalate to trusted protection bodies

Annex D: Security Incident Log

Date: _____ Time: _____

Location: _____

Journalist: _____

Role/Position: _____

Witnesses/Individuals involved: _____

Type of Incident:

- ☐ Verbal threat
- ☐ Online harassment
- ☐ Physical assault
- ☐ Police detention / intimidation
- ☐ Confiscation / destruction of equipment
- ☐ Data breach
- ☐ Attempt to access sources
- ☐ Other: _____

Immediate Consequences:

- ☐ Physical harm
- ☐ Emotional distress
- ☐ Loss of equipment
- ☐ Data breach
- ☐ Interference with work
- ☐ Other: _____

Factual Description of the Incident:

Actions Taken – Internal:

- ☐ Informed the editor
- ☐ Evidence collected
- ☐ Protection measures reinforced
- ☐ Psychological support
- ☐ Other: _____

Actions Taken – External:

- ☐ Complaint filed with police
- ☐ Contact with MFWA / UNESCO / LGDH
- ☐ Legal support
- ☐ Other: _____

Recommendations: _____

Signatures:

Journalist: _____

Safety Focal Person: _____

Date: ____ / ____ / ____

Annex E: Security Checklist for Sensitive Publications

1. Editorial Verification

- ☐ Information verified with ≥ 2 sources
- ☐ Confidential sources protected
- ☐ Documents authenticated
- ☐ No unnecessary personal data included

2. Risk Assessment

- ☐ Possibility of retaliation against the journalist?
- ☐ Risk to source/informant?
- ☐ Risk of incitement to hatred?
- ☐ Editor and Safety Focal Person consulted?

3. Language and Ethics

- ☐ Neutral language
- ☐ No defamation or unsubstantiated allegations
- ☐ No stereotypes
- ☐ Clear separation of facts and opinion

4. Digital Security

- ☐ Document protected and encrypted
- ☐ Sensitive files securely stored
- ☐ Communication with sources via secure channels
- ☐ Metadata checked/cleaned

5. Legal Review

- ☐ Compliance with the Press Law
- ☐ No violation of judicial secrecy
- ☐ No defamatory elements
- ☐ Legal opinion obtained (when necessary)

6. Final Approval

- ☐ Responsible Editor – approved
- ☐ Safety Focal Person – validated
- ☐ Management (for high-risk stories) – validated

