FANR
الهيئة الاتحادية للرقابة النووية
Federal Authority for Nuclear Regulation

United Arab Emirates

FANR's Whistleblowing System

F.A.Q

FANR
الهيئة الاتحادية للرقابة النووية
Federal Authority for Nuclear Regulation

United Arab Emirates

Table of Contents

(A) General Queries

1. What is the Report to Protect (R2P) System?

The “Report to Protect System" is FANR’s independently managed Whistleblowing System and constitutes one central hub of FANR for receipt of all whistleblowing concerns, including anonymous reporting of:

- Concerns related to Safety, Security and Safeguards (Non-emergencies).
- Fraud and misconduct concerns,

The R2P System allows FANR to:

- Protect the public and the environment from the harmful effects of ionising radiation and ensure the exclusively peaceful use of nuclear energy and radiation sources.
- Protect organization from the consequences of any wrongdoings, such as fraud and misconduct, and instil ethical culture instead,

2. Who is a whistle-blower?

A whistle-blower is any individual or organisation who raises a genuine concern in ‘good faith’ and discloses information of suspected wrongdoing or potential Safety, Security and Safeguards concerns to FANR.

3. What is whistleblowing?

Whistleblowing is the act of disclosing information relating to suspected wrongdoing or potential Safety, Security or Safeguards concerns, but not information disclosed maliciously, recklessly or for any personal gain.

What matters is that the individual discloses information about a wrongdoing or potential Safety, Security or Safeguards concerns that otherwise would not be known and hence whistle blowers’ reporting is crucial to detect and prevent different types of wrongdoing.

4. Who can report using the R2P channels?

The R2P channels can be used for reporting concerns by FANR’s current and former employees, suppliers, vendors, agents, representatives, consultants, contractors, sub-contractors, applicants, licensees current and former staff and contractors as well as other stakeholders, including the public.

5. Who manages FANR’s R2P System?

The system is independently managed with no interference from FANR executive management.

(B) Reporting queries

6. What are the channels established by FANR to report whistleblowing concerns?

Making a report is easy. You can report any concern(s) within the scope of the R2P System using any of the four channels mentioned below:

1. Web reporting portal with feedback facility - available at R2P.fanr.gov.ae
2. Dedicated email account – send an email to R2P@fanr.gov.ae
3. In person (direct) communication with Chief Audit Executive (CAE) – Meeting can be scheduled by sending an email to CAE@fanr.gov.ae OR you may approach any of FANR's Inspectors to report any safety, security and safeguards concerns.

7. Can I report anonymously?

All matters raised through the aforementioned four channels of the R2P System are subject to strict confidentiality guidelines regarding the identity of the whistleblower. The system allows two (2) levels of anonymity:

1. Disclose Identity – In this option, your contact details will be available only to the Chief Audit Executive and the designated investigation member from FANR.
2. Anonymous – In this option, you do not need to enter any of your contact details thereby allowing complete anonymity in case you do not feel comfortable sharing your identify.

In either option, no information about the whistleblower's originating PC/IP Address shall be collected or displayed in any form for reports made via email or web reporting form.

8. What language(s) can I use to report concerns?

You can report concerns either in English or in Arabic through any of the R2P reporting channels.

9. Can I report my concern(s) after FANR's working hours?

Yes, all our channels are available 24/7/365.

10. What happens if I do not know what category my concern falls under?

In case of any confusion on what category to report, please select "**I do not know/other type of concern**". We will review your submitted concern(s) and assign a category accordingly.

11. What happens if I fail to include enough information, or if I have only limited information?

The more information that you can provide, the more valuable your report will be. However, it is best to provide any information you have no matter how much or little they are.

In case, we require any further information, FANR's R2P System provides confidential messaging facility (feedback room) through which we will request additional information.

12. How do I submit supporting documents to support my reported concern(s)?

- In case you are using the web-reporting portal, you can attach supporting documents to your report before you submit your concern(s) online.
- In case of using the email reporting channel, you can attach supporting documents in the email that you are sending to R2P@fanr.gov.ae.
- In case of in-person reporting, you can submit your documents directly to the Chief Audit Executive.

13. How do I know that my report has been received?

All whistleblowers would receive confirmation or acknowledgement of receipt of the reported concern(s) and where applicable a unique secret code for tracking as explained below:

- Web portal: you can see the acknowledgement of receipt on the screen
- Email ID: you will receive acknowledgement of receipt by email.
- In-person: you will have direct acknowledgement of receipt by the Chief Audit Executive.

14. What happens after I report my concern(s)?

If you submit your concern via the web portal, you will get an acknowledgment of receipt, a unique security code and you will be asked to set a password to access your personal feedback room by visiting R2P.fanr.gov.ae and clicking on "Check status of my submitted concern"

However, if you report your concern(s) in person or by email, you will receive only an acknowledgment of receipt.

You can use the unique secret code and your password to access the feedback room in order to track the status of the case and communicate with FANR.

The concern(s) will be handled confidentially in order to proceed with the initial assessment, investigation and closure.

15. Who usually investigates the reported concern(s)?

Independence and objectivity are paramount to FANR's R2P System; hence, FANR's internal procedures set appropriate framework for independent investigations.

16. How do I follow up or check the status of the concern(s) I reported?

After submitting your concern(s), you will be able to view the status of your report, manage your report securely, discuss the concerns with the assigned team and request a status update even if you decided to remain anonymous.

This can be done by accessing your personal feedback room https://www.R2P.fanr.gov.ae and clicking on "Check status of my submitted concern" using your unique security code and the password you have already set.

17. Shall I use the Whistleblowing System to notify FANR of a wrongdoing, even if I may have committed/participated in the offence?

Yes, you can still use the Whistleblowing System even if you may have committed the offence.

(C) Safety, Security and Safeguards queries

18. What can be reported as Safety, Security and Safeguards concerns (Non-emergencies)?

Concerns related to Safety, Security and Safeguards raised by applicants, current and/or former licensee staff, licensee contractors and other stakeholders, including the public, on issues directly or indirectly associated with the conduct of all activities related to the peaceful, safe and secure uses of nuclear energy and radiation sources within FANR's mandate, which include, but are not limited to:

- Concerns about the Safety, Security or Safeguards of FANR regulated activities, including potential violations of FANR regulatory requirements or potential violations of the Federal Law by Decree No. (6) of 2009 Concerning the Peaceful Uses of Nuclear Energy,
- Wilful violations of legislative or regulatory requirements through deliberate actions,
- Work environment that discourage workers from raising Safety, Security or Safeguards concerns, or other matters related to FANR mandate, including wrongdoing or harassment, intimidation, retaliation and discrimination related to raising Safety, Security or Safeguards concerns,
- Radiological concerns or any other danger related to the health and safety of individuals and the public,
- Concerns related to safety and security culture,
- Inadequate environmental protection against ionising radiation hazards,
- Poor implementation of Safety, Security or Safeguards requirements or obligations,

Moreover, issues such as unsafe staffing levels, incorrect and/or falsification and/or ambiguity in documentation/records, inadequate qualifications are often viewed as causes for concern because they are critical to assurance of the safety, security and protection of the nuclear facility, radiation sources and the public.

19. Why should I report suspected Safety, Security and Safeguards concerns?

Whistleblowing serves as an effective tool to allow FANR to achieve its mission to ensure protection of the public and the environment from the harmful effects of ionising radiation, and to ensure the exclusively peaceful use of nuclear energy and radiation sources.

20. What information/data to include in reporting Safety, Security and Safeguards concerns by email?

We encourage you to provide us with as much information as possible, taking into account the following points when reporting your concern(s) by email:

- What are the details of the concern(s) and the activity involved?
- What is the potential Safety, Security or Safeguards impact?
- How long has the condition existed and long do you think in might last?
- How did you find out about the concern(s)?
- Do you think that an individual is deliberately putting Safety, Security or Safeguards at risk or violating FANR regulations or legal requirements? If so, please provide the name and designation of the said individuals?
- Are there individuals that FANR should contact for additional information? Please provide the names and contact information of those individuals.
- Can FANR have copies of any supporting documents or any evidentiary information that you may have? (please attach, if any)
- What records should FANR review to verify the concerns and where is the location of these records?

21. Am I allowed as an employee to disclose information about my entity?

Yes, if you reported a risk to the management and no action has been taken to rectify the situation.

22. What if my concern is an emergency?

Concerns about an immediate threat of physical harm or damage to property as well as nuclear or radiological Safety, Security and Safeguards emergencies should NOT be reported via the R2P System.

Any nuclear or radiological Safety, Security and Safeguards emergencies are to be reported immediately by dialling the toll-free emergency number 800 326 7999 (24 hours – 7 days a week) or by sending an email to rn.er@fanr.gov.ae

Any concerns involving an immediate physical threat to an individual on FANR's premises should be immediately reported to FANR's Internal Security by calling 02 651 7333, or sending an email to Internal.Security@fanr.gov.ae, or contacting the Security Control Room by dialing 02 651 6567.

(D) Fraud and misconduct queries

23. What could I report as fraud and misconduct concerns?

You can report cases of fraud and misconduct, and suspected incidents thereof, which include, but are not limited to, the following:

- Crimes and criminal behaviour by any of FANR employees,
- Violations by any FANR employee of laws or regulations that may result in a gain to the perpetrator and/or a third party or a loss to FANR or loss of public funds,
- Violations by any FANR employee of FANR's Code of Ethics and Professional Conduct,
- Deception by any FANR employee, in their professional capacity, of others to obtain any financial or in-kind benefits,
- Unjust treatment by any FANR employee, which may result in any gain to the perpetrator and/or a third party or a loss to FANR or loss of public funds,
- Intentional breaches by any FANR employee of internal controls, policies, or applicable regulations that may result in any gain to the perpetrator and/or a third party or a loss to FANR or loss of public funds,
- Manipulation or deception by any FANR employee in the use or presentation of FANR's financial statements,
- Any intentional unethical behaviour by any FANR employee, which may result in any gain to the perpetrator and/or a third party or a loss to FANR or loss of public funds,
- Misuse by any FANR employee of the FANR's property for personal gains,
- Abuse of authority,
- Illegally destroying or deleting government records by any FANR employee,
- Unauthorized disclosure of information, breach of confidentiality or data leakage by any FANR employee,
- Embezzlement or false accounting by any FANR employee,
- Corruption, offering or acceptance of bribes or kickbacks by any FANR employee,
- Allegations against any FANR employee,
- Potential undisclosed conflicts of interest by any FANR employee,
- Collusion of any FANR employee with stakeholders/vendors/ suppliers of FANR,
- Deliberate cover up by any FANR employee of any of the violations mentioned above.

24. Why should I report suspected fraud and misconduct?

Whistleblowing is important for fostering high ethical standards and principles of integrity and honesty and, therefore, essential for maintaining public confidence in an organisation and its operations. By blowing the whistle, you can contribute to preventing the possible escalation of misconduct and minimising the possible negative impact of the issue.

We all have a responsibility of acting in an ethical manner and letting FANR know through the R2P System if someone is not acting appropriately. Reporting a concern is in essence an opportunity for FANR avoid the negative consequences of any possible violation and carry out the necessary investigation to address the situation in a timely manner.

25. What information/data should I include when reporting fraud and misconduct concerns by email?

We encourage you to try to provide us with as much information as possible. Some points to guide you while drafting your email include:

- Please provide details of the type of fraud or misconduct you suspect is going on (e.g., time, date, place and name(s) of the person/people involved),
- Is there anyone else involved in the activity you are reporting? If so, please provide any information you have on that person's activities,
- Location of evidence and other witnesses,
- How and when you have found out about the incident, and any prior efforts to address the problem,
- Include any information that you believe is relevant may prove that a possible fraud may be happening, has happened, or is about the happen,
- Any financial impact, physical threats of violence/damage or potential for retaliation

(E) Confidentiality, security and anonymity queries

26. Shall my report and identity remain confidential?

All matters raised through the defined channels established under the R2P System are subject to strict confidentiality guidelines regarding the identity of the whistleblower.

Even if a whistleblower chooses to be identified, FANR will ensure that his/her identity will not be disclosed to anyone else apart from the authorized investigation team. Identity of the whistleblower will only be disclosed where legally necessary.

27. How does FANR protect my identity and assure my anonymity?

Measures taken to protect identity and assure anonymity include the following:

- The R2P System is supported by an independent service provider,
- In-person reporting is made directly to Chief Audit Executive who is independent from FANR Executive Management,
- The R2P System meets the highest security standards to prevent unauthorized access,
- All members of the team receiving any concern are subject to maintaining strict confidentiality guidelines regarding the identity of the whistleblower at all times.

Moreover, you do also have a responsibility to ensure that you do not disclose/discuss the information submitted to FANR.

28. Can anyone else login to see the concern(s) I have reported?

No, all secret code and passwords are unique. Once you set a password for your unique secret code, only you will be able to view your report. Unless you give someone your secret code and password, no one else can view your report.

29. What should I do if I forget the unique ID or password?

As part of our process to protect your identity, we do not provide a retrieval process for lost logins or passwords. So in case you forget the unique security code or password, it cannot be restored for security reasons and you will no longer be able to check the status of your report or use the feedback room. Hence, we encourage you to maintain your unique secret code and password securely.

However, you can submit a new report and refer to your original report to help us link the two reported concerns.

(F) Retaliation queries

30. Will I be retaliated against by FANR Management for reporting my concern?

FANR does not support retaliation in any form. We will ensure protection from retaliation, firing or any other harassment and exclusion in the workplace to any FANR employee who reports a suspected concern in good faith, even if the concern is not substantiated. To prevent retaliation against FANR employees, we will ensure keeping the whistleblower's identity confidential.

Furthermore, the Whistleblowing System specifically asks all whistleblowers at the time of reporting of any potential threats of retaliation in order to ensure adequate measures are taken to prevent perceived retaliation.

31. What should I do if I face retaliation by FANR Management for reporting my concern?

If an individual or organization learns the identity of a whistleblower who has reported evidence of their wrongdoing, they may think about taking a retaliatory action to discredit or punish the whistleblower. This is especially common when the accused has leverage over the whistleblower in the workplace.

FANR employees are requested to report immediately to the Chief Audit Executive any form of retaliation by FANR Management for reporting any concern(s). Since, FANR does not accept nor condone retaliation in any form; no type of reprisal against FANR employees will ever be tolerated.

32. What should I do if I am retaliated against by my entity (other than FANR) for reporting any concern(s) to FANR?

You can inform FANR while reporting your concern about any perceived threats of retaliation to enable us to address it during our investigation.

(G)Disclaimer

The material in this FAQ may not reflect the most current legal developments. The content and interpretation of the content addressed herein is subject to revision. We disclaim all liabilities in respect to the actions taken or not taken based on any or all the content of this FAQ.