JSC “Rogun HPP”

State Enterprise “Directorate for Flooding Zone of Rogun HPP”

Project Management Group for Energy Facilities Construction under the President of the Republic of Tajikistan

ROGUN HYDROPOWER PROJECT – UPDATED ENVIRONMENTAL AND SOCIAL IMPACT ASSESSMENT

Security Management Plan

JSC “Rogun HPP”

State Enterprise “Directorate for Flooding Zone of Rogun HPP”

Project Management Group for Energy Facilities Construction under the President of the Republic of Tajikistan

ROGUN HYDROPOWER PROJECT – UPDATED ENVIRONMENTAL AND SOCIAL IMPACT ASSESSMENT

Environmental and Social Impact Assessment

Security Management Plan

TYPE OF DOCUMENT (VERSION) PUBLIC

PROJECT NO. 70097413

OUR REF. NO. ESIA-VOL3-A7-SMP-REV01-ENGLISH

DATE: OCTOBER 2025

QUALITY CONTROL

CONTENTS

TABLES

FIGURES

TABLE OF ACROYMNS AND ABBREVIATION

Term	Definition
ADB	Asian Development Bank
AIIB	Asian Infrastructure Investment Bank
ALARP	As Low as Reasonably Practicable
AMSL	Above Mean Sea Level
AoI	Area of Influence
CASA	Central Asia-South Asia project
CoC	Code of Conduct
DSPoE	Dam Safety Panel of Experts
E&SPoE	Environmental and Social Panel of Experts
ECS	Environmental, Climate and Social
EDB	Eurasian Development Bank
EHS	Environmental, Health and Safety Guidelines
EIA	Environmental Impact Assessment
EIB	European Investment Bank
ERP	Emergency Response Plan
ESCP	Environmental and Social Commitment Plan
ESF	Environmental and Social Framework
ESIA	Environmental and Social Impact Assessment
ESMP	Environmental and Social Management Plan
ESP	Environmental and Social Policy
ESPOE	Environmental and Social Panel of Experts
ESHS	Environmental, Social, Health and Safety
ESS	Environmental and Social Standards
EU	European Union
GIIP	Good International Industry Practice

Term	Definition
HESG	Hydropower Sustainability ESG Gap Analysis Tool
HPP	Hydropower Project
IFAS	International Fund for the Aral Sea
ILO	International Labor Organization
IsDB	Islamic Development Bank
KFAED	Kuwait Fund for Arab Economic Development
NGO	Non-Governmental Organization
NTS	Non-Technical Summary
O&M	Operation and Maintenance
PAPs	Project Affected Persons
PIU	Project Implementation Unit
PMG	Project Management Group
PO	Project Owner
PPE	Personal Protective Equipment
RAP	Resettlement Action Plan
RCC	Gravity Roller Compacted Concrete Dam
SEP	Stakeholder Engagement Plan
SFD	Saudi Fund Development
TA	Technical Assistance
TMP	Traffic Management Plan
ToR	Terms of Reference
UN	United Nations
WB	World Bank
WBG	World Bank Group
WHO	World Health Organization

1. INTRODUCTION

1.1.1. The Rogun Hydropower Project (HPP) located in the Republic of Tajikistan, is currently undergoing an extensive phase of construction and partial operation, with two turbines already in active use. The Project is owned by the Rogun Open Joint Stock Company (JSC) (hereafter referred to as 'Rogun JSC') and managed by the Project Management Group (PMG) for Energy Facilities Construction under the President of the Republic of Tajikistan. Rogun JSC is responsible for overseeing both the construction and long-term operation of the Project.

1.1.2. This document is the Security Management Plan (SMP), developed as part of the Volume III, Environmental and Social Management Plan (ESMP) of the Environmental and Social Impact Assessment (ESIA).

1.1.3. The Security Management Plan is designed to ensure compliance with ESIA requirements and alignment with the ESMP and Environmental and Social Commitment Plan (ESCP). The SMP addresses security management within the Project boundaries and physical security measures necessary throughout the construction and operational phases, focusing on tangible asset protection while excluding cybersecurity considerations. This SMP serves as a framework to align Rogun HPP's security operations with international standards, ensuring comprehensive protection measures and fostering community trust and cooperation.

1.1.4. The Security Management Plan (SMP) in this document provides a structured framework to ensure the security of the Rogun HPP project while maintaining compliance with international standards such as ESS4 (Environmental and Social Standard 4) and Good International Industry Practice (GIIP). It establishes clear security governance and responsibilities, defining the roles of Rogun JSC, Contractors, and Security Providers to ensure accountability in security operations. The plan aligns with World Bank guidelines, emphasizing adherence to rights principles, proportional use of force, community engagement, and grievance redress mechanisms to mitigate risks effectively. SMP mandates training and awareness programs for security personnel, with a particular focus on screening procedures, de-escalation techniques, and interaction with vulnerable groups, including children. Additionally, this plan has been developed in compliance with the applicable laws of the Republic of Tajikistan and the Environmental, Social, Health, and Safety (ESHS) standards of the World Bank, along with standards of various international financial institutions (IFIs), collectively referred to as 'the Applicable Standards'. A detailed overview of the Applicable Standards is provided in **Volume 1, Chapter 02: Legislation and Standards** of this ESIA.

1.1.5. Rogun JSC shall be responsible for implementing, monitoring, and evaluating the effectiveness of this plan and any associated security management sub-plans developed for the Project.

1.1.6. In preparing this SMP, a comprehensive gap analysis and desktop review of the project Security Management Plan (Tractebel), was conducted, along with other documents provided by Rogun JSC security department. Additionally, a site visit was carried out in November 2024 to evaluate current security management on the construction site, assessing improvements to security practices and whether there is need to enhance security and efficiency.

1.2. SECURITY MANAGEMENT PLAN PURPOSE

1.2.1. The purpose of this Security Management Plan (SMP) is to set out security measures, actions, and strategies to be implemented by Rogun JSC and its contractors during both the construction and

operational phases of the Rogun Hydroelectric Power Plant (HPP) project. Developed in line with the World Bank's Environmental and Social Standard 4 (ESS4), which focuses on "Community Health and Safety," this plan is essential for safeguarding surrounding communities. The SMP addresses the potential security risks associated with the Rogun HPP project and its mitigation measures.

1.2.2. This plan applies to all buildings, offices, and construction sites under the control of Rogun JSC and its contractors. It includes key elements of a Security Management System (SMS) to ensure:

- A secure operational environment across all facilities and sites.
- Safety and security for communities, workers, and others who may be affected by Project security measures and security personnel.
- Ensure compliance with all applicable standards, frameworks, and guidelines outlined in the World Bank Environmental and Social Standards (ESS) and relevant regulations of the Republic of Tajikistan.
- Establish and maintain high standards of behavior and conduct for both military and non-military personnel in their interactions with the community. This includes ensuring respectful, ethical, and professional conduct at all times, fostering positive relationships, and minimizing any potential conflicts or security risks.
- The Security Management Plan (SMP) ensures compliance with the requirements of the World Bank ESF and Good International Industry Practice (GIIP) by implementing security measures that prioritize the protection of people's rights, community safety, and risk mitigation. The ESF emphasizes the need for security arrangements that avoid harm to workers and local populations. The SMP integrates GIIP by establishing clear guidelines on the use of force, security personnel conduct, and risk assessment methodologies. It includes training programs on de-escalation, conflict resolution, and gender-based violence (GBV) prevention, ensuring security personnel operate within ethical and legal boundaries.

1.3. SITE-WIDE SMP COMPLIANCE FRAMEWORK

1.3.1. All Contractors and Security Suppliers are and shall continue to comply and align with the specific requirements outlined in this Plan. Regular assessments/reviews/drills shall be conducted to ensure continuous compliance, with guidelines provided for adherence. Deviations from the SMP requirements must be reported promptly, with established procedures for correction and prevention. Legal compliance is integral, and standards must be in place to monitor and adapt to evolving legal and regulatory obligations. Compliance requirements are:

1.3.2. • Ensure all security measures align with World Bank Environmental and Social Framework (ESF) and Good International Industry Practice (GIIP).

1.3.3. • Prevent and mitigate risks to workers and the community.

1.3.4. • Conduct thorough background checks and screening of security personnel before deployment.

1.3.5. • Provide mandatory training in legal rights, use of force, conflict de-escalation, and gender-based violence (GBV) prevention.

1.3.6. • Special training on screening and engagement with vulnerable groups, including children and displaced community members.

1.3.7. • Implement strict guidelines on the proportional use of force, in compliance with UN Basic Principles on the Use of Force and Firearms.

1.3.8. • Prohibit excessive force, arbitrary detention, and use of weapons beyond defined security threats.

1.3.9. • Establish a grievance redress mechanism (GRM) that allows safe and confidential reporting of security-related complaints.

1.3.10. • Conduct regular community liaison meetings to address security concerns and maintain transparency.

1.3.11. • Ensure all security incidents, including alleged misconduct, are documented and reported.

1.3.12. • Security contractors must liaise with Rogun JSC for threat assessment briefings and update security threat risk assessments accordingly.

• Ensure security patrols and surveillance measures are conducted without disrupting operational or community activities.

1.3.13. All Contractors shall conduct a gap analysis between this Security Management Plan and their existing Security Management Plan or Site Security Plan. The gap analysis enables Contractors to formulate a plan to address any identified gaps, ensuring timely compliance with this Security Management Plan. Each contractor's draft plan should be provided to ER/PMC for review and approval.

1.3.14. All Contractors shall adhere to all local, regional, or national regulations as a minimum requirement. Additionally, it shall identify and incorporate any necessary approvals, licenses, and permits from local authorities into this Security management system.

1.4. SUPPORTING PLANS

1.4.1. The following plans and documents support the Security Management Plan and should be read in conjunction with this document to ensure a coordinated approach to security, compliance, and site management:

- Volume 1: Environmental and Social Impact Assessment
- Volume 3: A01 Environmental and Social Management Plan (ESMP);
- Volume 3, A09: Traffic Management Plan;
- Volume 3: A08: Community Health and Safety Plan
- Volume 3: B12: Emergency Preparedness and Response Plan;
- Volume 3: B13: Occupational Health and Safety Management Plan; and
- Volume 3: C1: Contractor Management Plan.

1.5. SUPPORTING APPENDICES

1.5.1. The following annexes provide supplementary tools and resources to support the implementation and monitoring of the SMP. Please note these annexes may or may not be finalised and included in this SMP deliverable.

- *Appendix A – Security Threat Risk Assessment*
- *Appendix B –Site Security Plan (Minimum Contents)*
- *Appendix C – SSP Compliance Checklist*
- *Appendix D – Supplier Site Security Instructions*
- *Appendix E – SSI Compliance Checklist*
- *Appendix F –Security Incident Report*
- *Appendix G – Site Security Review*
- *Appendix H – Monthly Security Incident Report*
- *Appendix I – Security Role Requirements*
- *Appendix J – Accommodation Camp Acceptable Behaviour*
- *Appendix K – Site Suitability Assessment Report Template*
- *Appendix L – Chain Link Fencing and Detail (US Department of Defence Ufc 4-022-03 1 October 2013 Unified Facilities Criteria Security Fences & Gates)*
- *Appendix M – Chain Link Swing Gate and Details (US Department of Defence Ufc 4-022-03 1 October 2013 Unified Facilities Criteria Security Fences & Gates)*

1.6. REPORT STRUCTURE

Table 1-1 – Report Structure

Section	Name
1	Introduction
2	Applicable Standards and Guidelines
3	Site Conditions
4	Roles And Responsibilities
5	Stakeholder Engagement and Coordination
6	Security Process
7	Site Security
8	Site Access Control
9	Site Access Control – Vehicles

10	Security of the Powerhouse
11	Security Control Room and Centralised Monitoring Room
12	Security Of Construction Equipment and Materials
13	Office Security
14	Personnel Security During Construction
15	Explosive Handling
16	Training, Awareness and Exercises
17	Security Personnel - Code of Conduct
18	Security Threat Risk Assessment
19	Use of Force
20	Assessing Allocations or Incidents Related to Security
21	Emergency And Incident Management
22	Emergency Response plan
23	Security and Traffic Coordination
24	Training, Awareness and Exercises
25	Security Personnel – Code of Conduct
26	Use Of Force
27	Security And Traffic Coordination

2. APPLICABLE STANDARDS AND GUIDELINES

2.1.1. This document has been informed by key regulatory requirements and aligns with principles from essential guidance documents, including national and international standards and best practices that support security management, as well as community and environmental risk management considerations:

Tajikistan Law, including International Agreements to which Tajikistan is a Party:

2.1.2. Law on Safety, Republic of Tajikistan (2011)

2.1.3. Labor Code (2016)

2.1.4. Code of Administrative Violations (2010)

2.1.5. Criminal Code of the Republic of Tajikistan

2.1.6. The Law on Public Meetings, Demonstrations and Rallies (2014)

2.1.7. The Law on Emergency Response Services, Emergency Rescue Teams and Rescue Worker Status;

2.1.8. The Law on Control of Civil Purpose Explosives

- Law Of the Republic of Tajikistan on Combating Terrorism

World Bank Environmental and Social Framework (ESF) Standards:

- Environmental and Social Standard 1 (ESS1): Assessment and Management of Environmental and Social Risks and Impacts
- Environmental and Social Standard 2 (ESS2): Labour and Working Conditions
- Environmental and Social Standard 4 (ESS4): Community Health and Safety

World Bank Guidelines and Notes:

- General Environmental, Health, and Safety (EHS) Guidelines (2007): Section 3.0: Community Health and Safety
- Guidance Note for Borrowers: Environmental & Social Framework for IPF Operations – ESS4: Community Health and Safety
- Good Practice Note on Security Personnel

Asian Development Bank (ADB) Environmental and Social Framework (ESF) (September 2024)

The Voluntary Principle on Security and Human Rights

UN Code of Conduct for Law Enforcement Officials

ISO 31000:2018: Security Risk Management

Asian Infrastructure Investment Bank

European Investment Bank (EIB) Standards (2013) and **European Union Directives** as they apply to security.

3. SITE CONDITIONS

3.1. SITE LOCATION

3.1.1. Detail on the site location and project background is provided within the **Volume 1, Chapter 1: Introduction** and **Volume 1, Chapter 3: Project Description** of this ESIA.

3.2. SITE DESCRIPTION AND KEY FEATURES

3.2.1. Detail on the project description and site components is provided within the **Volume 1, Chapter 3: Project Description** of this ESIA.

3.3. KEY SECURITY MANAGEMENT AREAS

3.3.1. This SMP addresses critical areas essential for both the construction and operational phases of the Rogun HPP. Given the site's mixed-use status, with construction activities occurring alongside operational functions, the SMP incorporates adaptable strategies to ensure controlled and efficient security management.

Security management areas for the Rogun HPP project include critical zones requiring specific security measures to address risks related to people from those who are responsible for preventing unauthorized access, sabotage, and safety. These areas are:

3.3.2. **Construction and Operational Zones**: Active areas where construction, assembly, and operational activities take place, including the dam and substations.

3.3.3. **Workers' Camps:** Housing facilities for workers, including dormitories and communal areas. These camps require security to manage access, prevent unauthorized entry, and address potential incidents such as theft, harassment, or unrest.

3.3.4. **Site Access Points:** Main and secondary gates for personnel, vehicles, and material transport. Security measures include identity verification, vehicle inspections, and work permit checks.

3.3.5. **Underground Roads and Tunnels:** Subsurface routes used for material transport and access to critical facilities.

3.3.6. **Perimeter Security:** Includes fencing, check posts, and areas monitored by the national military. The porous perimeter due to surrounding hills requires additional measures, including air surveillance and patrols.

3.3.7. **Parking and Equipment Staging Areas:** Spaces for vehicle parking, material storage, and equipment maintenance.

3.3.8. **Pedestrian and Worker Transit Zones:** Pathways, walkways, and pick-up/drop-off points for workers moving around the site. These areas need adequate security and monitoring to manage risks associated with mixed-use traffic zones.

3.3.9. **Villager Access Areas:** Zones where villagers still reside or interact with the project due to the ongoing resettlement process.

4. ROLES AND RESPONSIBILITIES

4.1.1. The effective implementation of this SMP relies on a site-wide understanding of security roles and responsibilities across all project activities and personnel.

4.1.2. Rogun JSC, as the overseeing entity, holds ultimate responsibility for SMP enforcement and alignment with the Project's ESMP and other applicable standards. The Project Management Consultant (PMC), acting as the Employer's Representative, supports by conducting regular audits, approving contractor-specific SMPs, and reinforcing site-wide compliance with security management protocols.

4.1.3. Rogun JSC holds ultimate responsibility for implementing the requirements of this SMP across all project activities, supported by the Employer's Representative (ER) / Project Management Consultant (PMC). The ER/PMC shall provide regular compliance checks, approve Lot-specific SMPs, and ensure site-wide adherence to each chapter's minimum requirements and best practices. Contractors are required to align their operations with the guidelines outlined in each section of this SMP.

4.1.4. Detail on the Organisational Structure of the Rogun HPP Project is provided within the **Volume 1, Chapter 1: Introduction** and **Volume 1, Chapter 3: Project Description** of the ESIA

4.1.5. The following **Table 4-1** provides indicative breakdown of key roles and responsibilities. As project activities progress, this table may be updated to ensure responsibilities remain relevant and effective.

Table 4-1 - Roles and Responsibilities

Role	Responsibilities
Project Management Group for Energy Facilities Construction under the President of the Republic of Tajikistan (PMG)	The PMG holds high-level authority over the Rogun HPP Project, overseeing its alignment with overarching project objectives, compliance with national and international standards, and adherence to lender requirements. Key responsibilities include: Providing strategic oversight to ensure compliance with the ESMP and the Environmental and Social Commitment Plan (ESCP). Approving significant updates and changes to Project documentation to maintain alignment with evolving site conditions and operational requirements. Allocating adequate resources to support the successful implementation of this SMP across all project phases. Integrating security management responsibilities into the Project's broader operational framework to enhance site-wide compliance and safety.
Rogun JSC	Rogun JSC serves as the client and on-site project authority responsible for overseeing security management and approving the SMP. Key responsibilities include: Developing and disseminating the SMP within three months of the effective date, establishing baseline security requirements and responsibilities for all contractors.

Role	Responsibilities
	Reviewing, approving, and implementing the SMP, ensuring alignment with Project objectives and ESIA requirements. Maintaining control over security measures and enforcement through the Security Department. Ensuring alignment of all contractor-specific Site Security Plans with the SMP and applicable standards. Conducting regular on-site audits and inspections to assess SMP compliance, with findings reported to the PMG as necessary. Collaborating with the ER/PMC and other stakeholders to monitor and mitigate security-related risks.
Security Department (Rogun JSC)	As an arm of Rogun JSC, the Security Department oversees SMP compliance. Responsibilities include: Managing access control and enforcing SMP protocols for all vehicles and personnel on-site. Enforcing SMP requirements through direct actions, with the authority to issue warnings, suspend security personnel authorisations, and recommend further actions, including notices of non-compliance, to employers. Operating the on-site CCTV system to monitor vehicle access, pedestrian access, and identify non-compliance or hazards in real time. Issuing warnings, suspending security personnel authorisations, and recommending disciplinary actions for SMP violations. Conducting regular security briefings and coordinating with contractors to address security management issues. Collaborating with ER/PMC and contractor HSE teams to ensure that security measures and security protocols are effectively implemented and enforced.
Project Management Consultant (PMC) (*Employer's Representative – Tractebel)*	Acts as the Employer's Representative, ensuring contractors' compliance with SMP standards. Responsibilities include: Reviewing and approving contractor-specific SMPs in coordination with Rogun JSC, ensuring each plan aligns with the overarching SMP and facilitating final approval within six months of the effective date for relevant Lots. Conducting security personnel security training, providing on-site security briefings, and reinforcing "rules of use of force" compliance among security personnel. Auditing site security and security personnel qualifications, including site access logs, security control room recordings, and material gate pass, to ensure contractor adherence to established standards. Performing compliance audits and site inspections to monitor SMP adherence across contractors, with special attention to high-risk areas. Providing security briefings and training resources to contractors, supporting their implementation of security practices.

Role	Responsibilities
	Coordinating with Rogun JSC and the Security Department to address compliance issues, mitigate security risks, and resolve operational challenges as they arise.
National Military in coordination with Rogun JSC security department	The National Military is responsible for securing the project perimeter, including establishing and maintaining fencing, gates, and other barriers. The National Military staff control all primary access points to the project site. This includes conducting thorough checks and patrols to prevent unauthorized access. Military checkpoints are set up around strategic areas to control and monitor movement, ensuring only authorized personnel and vehicles enter sensitive zones. The National Military presence is a key deterrent to potential threats, providing a high level of physical security and rapid response capability for perimeter breaches
Site Contractors *Project Contractor Group* (PCG) (e.g., WeBuild, Ariana, TGEM, EMZ, Voith)	Site Contractors include all contractor entities operating on-site, collectively responsible for implementing SMP requirements, conducting the gap analysis, developing their own Security Plans in alignment with this SMP within their designated work areas. Responsibilities are grouped as follows: **Primary Contractors** Develop and submit detailed contractor-specific Site Security Plan tailored to their work scope, ensuring alignment with the overarching SMP requirements. Train all personnel on SMP protocols, including site access control, security of site, security control room duties. **Project Managers:** Hold overall responsibility for SMP implementation within their designated areas. Ensure adequate resources (e.g., barricades, LED lights, tower lights) are available to support security. Collaborate with the Security Team to enforce SMP requirements and align with Project Security standards. **Supervisory Staff (e.g., Plant Managers, HSE Team, Site Supervisors):** Appoint qualified supervisors to oversee daily SMP implementation, ensuring compliance with protocols. Conduct security checks and equipment inspections to uphold operational security standards. Monitor security personnel behaviour, address non-compliance issues, and implement corrective actions as needed. **Subcontractors** Ensure full compliance with the SMP for all subcontracted teams, clearly communicating specific security management protocols and enforcing adherence within designated work areas.

Role	Responsibilities
	Liaise and coordinate security arrangements with Primary Contractors to maintain unified and effective security management.
Private security Sub-contractors	Private security subcontractors engaged on the project shall play a vital role in maintaining site safety, protecting personnel and assets, and supporting the overall implementation of the Security Management Plan (SMP). Their responsibilities must be clearly defined, contractually agreed upon, and aligned with national laws, international standards (e.g., UN Voluntary Principles, ICoC, ESS4), and the site-specific security requirements. The following outlines the key roles and responsibilities of Private Security Subcontractors: • Ensure all security personnel are properly recruited, with thorough background checks and vetting processes in place to confirm identity, qualifications, and absence of prior misconduct or criminal behaviour. • Deliver or facilitate all mandatory training before deployment • Deploy only trained, uniformed, and authorized personnel in accordance with approved rosters and duty posts. • Maintain discipline, professionalism, and respectful conduct at all times, especially when engaging with the public or community members. • Ensure adherence to the Code of Conduct, including zero-tolerance for harassment, abuse, or discrimination. • Provide a dedicated supervisory team to oversee day-to-day security operations, manage shift scheduling, monitor compliance, and address performance issues. • Maintain effective communication with the Contractor's site security lead and Rogun JSC. • Implement security tasks and procedures in accordance with the SMP, Site Security Plan (SSP), and Site Security Instructions (SSI). • Support the implementation of site-specific measures, including access control, perimeter surveillance, incident response, and emergency evacuation protocols. • Promptly report all incidents, including suspicious activity, breaches, accidents, or allegations of misconduct, using established reporting formats. • Inform all personnel about internal and external grievance mechanisms, including confidentiality guarantees and whistleblower protection. • Encourage the reporting of misconduct and ensure non-retaliation policies are upheld. • Ensure all issued equipment (e.g., radios, batons, body cameras if applicable) is functional, maintained, and used appropriately. • Coordinate with military, police, and other actors in line with civil-military cooperation protocols and chain-of-command instructions.

Role	Responsibilities
	• Maintain up-to-date personnel files, training records, duty rosters, incident logs, and performance evaluations.
Government Authorities **(Local Police and authorities)**	Public Security forces (local police and authorities) are responsible for responding to and investigating any criminal activity within the vicinity of or involving the project site. Public Security forces maintain the primary role in managing any civil disturbances, demonstrations, or public order incidents that may affect the project. Public Security can be called upon to assist Rogun JSC and the National Military during emergencies, including large-scale security events, to ensure a swift and effective response. Public Security's involvement ensures that any criminal or civil issues are handled in accordance with national laws and regulations.

5. STAKEHOLDER ENGAGEMENT AND COORDINATION

5.1. SITE-WIDE ENGAGEMENT AND PARTICIPATION

5.1.1. Site-wide participation at all levels is essential for the effective implementation of this SMP and the achievement of project-wide security management objectives. Rogun JSC, the ER/PMC, contractors, and the community should each engage in open communication, collaboration, and adherence to the established standards, ensuring a unified approach to security across the project.

Contractor Coordination

5.1.2. Contractors play a central role in SMP implementation within their respective work areas. Rogun JSC and the ER/PMC are facilitating and shall continue to facilitate regular coordination meetings with contractors to address SMP updates, review compliance, and discuss corrective actions as necessary.

5.1.3. Key coordination activities include:

- **Regular Contractor Meetings:** Conducting meetings, e.g., monthly, led by Rogun JSC or the ER/PMC, to discuss SMP updates, security arrangements adjustments, and any incident findings that may impact ongoing operations.
- **Contractor Feedback Loops:** Establishing feedback channels for contractors to raise security-related concerns, suggesting improvements, and reporting on-site security issues. This input shall be reviewed and integrated into SMP revisions where applicable.
- **Communication Protocols:** Defining and communicating reporting lines for security incidents and near-misses, ensuring timely communication between contractors, Rogun JSC, and the ER/PMC to support unified and effective responses to security related issues.

5.2. COMMUNITY ENGAGEMENT AND SECURITY RISK MITIGATION

5.2.1. **Volume 3: A13: Stakeholder Engagement Plan (SEP)** sets out the management of community engagement and security risk mitigation and integration.

5.2.2. Engaging with the surrounding community is essential to address potential security risks, particularly in areas where the project may intersect with local communities and shared spaces. Rogun JSC is working closely with community representatives to mitigate risks and ensure safe and cooperative interactions between the project and the public. Community engagement activities include:

5.2.3. **Public Safety Briefings:** Periodic safety briefings to update communities on anticipated security measures, high-risk areas, and any temporary restrictions or safety protocols implemented around the project site.

5.2.4. **Feedback and Grievance Mechanisms:** Grievance mechanisms have been established for complaints about the project, as well as for complaints by workers at the project site. Responses to grievances are documented, with corrective actions initiated promptly to address valid concerns.

5.2.5. **Awareness Outreach:** The project is implementing security awareness outreach near villages and public spaces. These campaigns educate the community on recognizing potential security threats, understanding the project's safety protocols, and knowing how to report suspicious activity or incidents.

5.3. GOVERNMENT AND REGULATORY COORDINATION

5.3.1. Effective coordination with government authorities is essential to ensure the safety and security of the Rogun HPP project, its personnel, and infrastructure. This section outlines the responsibilities of relevant government entities and establishes mechanisms for collaboration between Rogun JSC and national security and regulatory bodies. This collaboration can be done by creating and launching regular interactions at suitable levels with each party, encompassing both formal and informal conversations, consultations, reporting, and information exchange. These specific activities will focus on regularly collection of feedback from stakeholders and pinpointing areas that may need improvement to enhance security practices.

Mechanism of Coordination

5.3.2. Formal Agreements and MoUs:

A Memorandum of Understanding (MoU) shall be signed between Rogun JSC and the Ministry of Defense, outlining the scope of engagement, command hierarchy, restrictions on use of force, legal rights obligations, and procedures for reporting and accountability. Similar engagement terms may be developed with the Ministry of Internal Affairs and other relevant bodies.

5.3.3. Appointment of Security Liaison Officers:

A government liaison officer, preferably from the Ministry of Defense, shall be embedded to ensure real-time coordination between military units and the project's internal security team.

5.3.4. Regular Coordination Meetings:

Monthly or bi-monthly coordination meetings shall be held with representatives from MoD and local authorities. These meetings shall review security incidents, community concerns, deployment adjustments, and training needs.

5.3.5. Incident Reporting and Response Protocols:

A standardised protocol shall be agreed upon for reporting incidents involving government forces. This includes an obligation to report to both the government chain of command and Rogun JSC security leadership. Government forces must seek project-level authorization for any non-routine deployments or operations on-site.

5.3.6. Legal and Disciplinary Framework:

In case of alleged misconduct by government personnel, Rogun JSC should work with appropriate ministries to trigger internal investigations, while also ensuring independent review by the Security Incident Oversight Committee. Outcomes must be shared with project stakeholders.

Coordination with National Military

5.3.7. The national military plays a critical role in securing the perimeter and addressing high-risk security scenarios such as sabotage, terrorist attacks, or vehicle-as-weapon attacks.

Responsibilities of the National Military:

5.3.8. Responsibilities of the national Military:

- Maintain continuous surveillance and patrols along the project's perimeter.
- Monitor and manage access points to prevent unauthorized entry.

- Deploy rapid response teams in case of high-risk incidents such as terrorist threats, explosions, or assaults.
- Provide tactical support during emergencies, including neutralizing threats and safeguarding critical infrastructure.
- Collaborate with project security teams to share intelligence on potential threats.
- Participate in joint drills and simulations to ensure seamless operational alignment.

Coordination with Police and Law Enforcement

The local police and public security forces are key partners in maintaining law and order around the project site and addressing incidents involving criminal activity or community-related issues.

Responsibilities of the Police:

Responsibilities of the police include:

- Investigate incidents such as theft, harassment, and other unlawful activities.
- Manage and respond to cases of trespassing, vandalism, or any violation of local laws.
- Address civil unrest, demonstrations, or protests near the project site.
- Mediate conflicts between the project and local communities to maintain harmony.
- Collaborate with Rogun JSC security teams to conduct joint investigations.
- Ensure a swift and lawful resolution to incidents involving both project personnel and community members.

Responsibilities of Government Authorities

5.3.9. Government authorities play an overarching role in ensuring that security operations align with national laws and international standards. Their responsibilities include:

- Developing and enforcing security regulations applicable to large-scale infrastructure projects like Rogun HPP.
- Conducting periodic inspections of the project site to ensure compliance with safety and security protocols.
- Allocating resources, including personnel, equipment, and vehicles, to support emergency response efforts.
- Providing training and capacity-building programs for both public and private security personnel.
- Facilitating information exchange on potential threats, including terrorism or sabotage.
- Establishing a central coordination mechanism between national security agencies and Rogun JSC.
- Prosecute offenders involved in unlawful activities related to the project.
- Providing guidance on the legal framework for addressing community grievances and compensation disputes.

- Establishing a task force comprising representatives from Rogun JSC, national military, police, and regulatory authorities.
- Holding regular meetings to discuss emerging threats, incident reports, and risk mitigation strategies.

5.4. STAKEHOLDER COMMUNICATION AND FEEDBACK INTEGRATION

5.4.1. Rogun JSC, supported by the ER/PMC, is establishing structured feedback loops to capture insights from contractors, community members, and government authorities. These inputs shall inform the SMP updates and ensure that security management practices evolve in response to stakeholder needs.

5.4.2. Formal communication procedures shall be implemented to document and communicate any significant SMP adjustments to contractors and the community. Key points include:

- All stakeholder communications, feedback, and corrective actions should be documented and reported as part of routine SMP monitoring.
- Significant SMP revisions or new security management protocols shall be communicated to contractors and community stakeholders through structured notifications, ensuring alignment with updated standards.

6. MANAGING SECURITY RISKS AND COMMUNITY IMPACT OF SECURITY PERSONNEL

The deployment of security personnel, including the Tajikistan Army, in the Rogun HPP project is essential for maintaining site security. However, their presence also presents potential risks to the local community, project staff, and overall operational integrity. To ensure that security operations align with international standards, World Bank guidelines, and project-specific security objectives, a structured risk management approach is necessary.

This section outlines key measures to mitigate risks associated with security personnel and their interactions with the community. The primary focus areas include comprehensive training and awareness programs, responsible use of force, community engagement initiatives, effective grievance mechanisms, and rigorous procedures for assessing allegations against security personnel. These measures are designed to promote accountability, build community trust, and prevent security-related misconduct.

6.1. TRAINING, AWARENESS AND EXERCISES

The site shall determine the training and competency requirements through Training Needs Analysis (TNA) that covers all levels of staff including senior management. The overarching training plan for security staff should have the following specific aims:

1) Ensuring all staff are adequately trained to complete their duties before the commencement of any shift. This also includes briefings to prepare them for known shift occurrences.
2) Providing continual professional development to improve the year-on-year service standards, site safety and site security standards.

Audits conducted by Rogun JSC shall assess the trained standard of security staff. The requirements should be specified by the Contractor to the Security Supplier through compliance to the SMP. The Security Supplier shall be responsible for developing the training and exercise plan for agreement with the contractors.

Given their differing mandates and capabilities, training requirements and responsibilities are distinguished below to ensure tailored delivery, operational clarity, and compliance with international standards.

Training Requirements for Private Security Personnel
Contracted private security guards under the responsibility of contractors.
Training Topics:

- Use of force and rules of engagement
- Site-specific threat and risk awareness
- Conflict de-escalation and crowd control
- Protection of civilians and infrastructure
- Cultural sensitivity and communication with community members
- Prevention of gender-based violence, sexual exploitation and abuse, and sexual harassment (GBV/SEA/SH)
- Grievance mechanisms and reporting obligations
- Laws, regulations and rights
- Relevant local laws and penalties

- Consequences of non-compliance
- Internal and external grievance mechanisms (hotlines, grievance mechanisms)
- Whistleblower protection & confidentiality

Responsible Party:
Contractors are responsible for ensuring all private security personnel receive this training prior to deployment and refresher training.

Training Requirements for Military Personnel
Training Topics:
- Site-specific security context and threat environment
- Use of force in accordance with international law
- Civil-military interaction and protection of civilians
- Community relations and avoidance of intimidation
- International standards on the use of firearms (e.g., UN Basic Principles)
- Prevention of GBV/SEA/SH and misconduct accountability
- Incident reporting and coordination with civilian stakeholders
- Relevant local laws and penalties
- Consequences of non-compliance
- Internal and external grievance mechanisms (hotlines, grievance redress systems)
- Whistleblower protection & confidentiality

Responsible Party:
The Ministry of Defense will deliver a tailored pre-deployment training program to all assigned military personnel. This training shall be conducted at an agreed military facility or on-site prior to assuming security duties, with refresher training provided biannually.

Onboarding

The On-Boarding training package should be submitted to Rogun JSC and the Contractor for approval within 4 weeks of being awarded the contract for the site. All security personnel shall undertake:

- Briefing, and where applicable, practice of the delivery requirements outlined in this schedule. This should include all relevant detail from:
  1) The Security Management Plan (SMP).
  2) Site Security Instruction (SSI).
  3) Site familiarisation tour.
  4) Customer service training and the standards required.
  5) Conflict management.
- In detail, the code of conduct expected of every security individual. Each employee should sign to indicate they have understood the specific requirements.
- Uniform issue, standards of turnout and cleanliness required.
- A specific session should be undertaken on HSE, and the emergency/incident response procedures for the site, and the individual's part in it.
- Basic and advanced first aid training, dependent upon the individual's starting knowledge.
- Fire extinguisher training, including identification of different extinguishers.
- Security of their Identification Card.

- Role based training on the site security infrastructure for all systems.

Annual Training Requirements

All security personnel shall undertake:

- Refresher and follow-on training on customer service.
- Refresher training on conflict management.
- Remedial training as required where improvements can be made.
- Refresher first aid training.
- Follow-on first aid training to increase the knowledge base of the security staff. This may be targeted to a more limited number of staff for more advanced techniques.
- Annual first aid training should include the use of vital life-saving equipment such as defibrillators.

Specialist Training Requirements

Selected security personnel shall undertake:

- Vehicle search training – ratio of least one trained operator per gate shift.
- Camera operator training – number based upon SCR staffing requirements.
- More advanced first aid training – 10% of security staff.

Training on Sexual Harassment and Gender-Based Violence

All security personnel, including contracted security staff and military forces, shall undergo mandatory training on GBV/SEA/SH to ensure a zero-tolerance approach. Key Training Components:

- Definition & Recognition of GBV/SEA/SH
- Understanding types of harassment (verbal, physical, psychological).
- Identifying early warning signs and risk factors.
- Legal implications and rights.
- Code of Conduct & Ethical Responsibilities
- Professional conduct when interacting with colleagues, site personnel, and civilians.
- Strict adherence to zero-tolerance policies on harassment.
- Reporting and Response Protocols.
- Proper channels for reporting GBV incidents while ensuring victim confidentiality.
- Security personnel's responsibility in responding to GBV cases.
- Victim Support & Response Training.
- Procedures for assisting victims of harassment or violence.
- Collaboration with law enforcement and victim support services.

Training on screening and scanning of children

Security personnel at the Rogun HPP site should receive specialized training in non-intrusive screening, cultural sensitivity, child protection, and conflict de-escalation. This ensures professional, respectful interactions, adherence to laws, regulations and rights standards, and the prevention of discrimination or harassment to maintain community trust. This training will help them provide reassurance and guidance, which can alleviate any distress children might feel during the screening process. Key training component shall include:

- Definition & Recognition of harassment against children
- Understanding types of harassment (verbal, physical, psychological).
- Identifying early warning signs and risk factors.
- Legal implications and rights standards.
- Code of conduct, respect and professionalism.
- Use of procedures to search the children's belongings.
- Parental presence if a pat-down is necessary and shall be conducted in manner that keeps the child comfortable.
- Clear and gentle communication with children.
- Reporting and Response Protocols.
- Proper channels for reporting harassment/ misbehaviour incidents against children while ensuring victim confidentiality.
- Security personnel's responsibility in responding to harassment/misbehaviour cases against children.
- Child Support & Response Training.
- Procedures for assisting child victims of harassment or violence.
- Collaboration with law enforcement and child support services.

Training Exercises

Security training exercises should be planned where a resulting security incident would be safety critical. Therefore, the following potential incidents should be exercised at least annually:

- Emergency evacuation of the site, including the use of muster areas and accounting for all personnel on the site.
- Emergency evacuation of accommodation sites, including the use of muster areas and accounting for personnel. This should include night-time exercising when the site is at its most vulnerable.
- Security incidents at the main entrance gate, including immediate action drills, control of internal traffic and people approaching the gate, control of external traffic and people approaching the gate and alternative access procedures.
- A bomb threat at a known and unknown location.
- A medical emergency with the injury of at least 5 personnel following a significant incident on-site. This should include the simulation of 'lifesaving' first aid and evacuation to either local medical assistance and/or medical evacuation.
- A breach of the site perimeter

Shift briefing

6.1.1. As part of the daily working routine all oncoming security personnel shall attend a 10 – 15 minute 'Shift briefing' prior to commencing their operational shift.

6.1.2. Shift briefings should be conducted by the relevant supervisor or manager and aim to cover topics where frequent reminders are useful to the ability of security personnel to conduct their activities. These may include:

1) Specific risks or activities relevant to the shift, including unique occurrences at the site.

2) Previous incidents in the last 24hrs, and indicators to be aware of for similar incidents occurring during their shift. This should include the most effective immediate action to be taken.
3) Reminder of a security standard operating procedure (SOP).
4) Refresher training on a first aid technique, evacuation or critical life safety aspect of the site. For example, as the site is next to the reservoir or river, then prevention of drowning techniques.

Competency Assessments

6.1.3. The personnel employed by the Contractor and Security Supplier should demonstrate the necessary competencies required for their respective roles. For certain key positions, the qualifications and experience required should be explicitly defined to ensure suitability for the responsibilities involved. Base-level competencies should align with the standards specified in this schedule, with particular emphasis on compliance with the Onboarding and Training requirements.

6.1.4. Training records should be maintained for all security personnel, covering their initial training and annual training. Each record shall be individual and may be subject to audit. Each session of training undertaken should be recorded with the following minimum details:

1) Training title.
2) Training duration.
3) Date of training.
4) Outcome of any assessment or attendance confirmed.
5) Name of the trainer or accreditation organisation.

Experience and Qualifications

Security roles should only be filled by individuals with suitable experience and knowledge. These apply to the following roles:

1) Site Security Manager.
2) Security Supervisor.
3) Security Control Room Supervisor.
4) Security Guard.
5) Security Control Room operator

(a). The minimum requirements are detailed in **Appendix I** – Security Role Requirements.
(b). Both Contractor and Security Supplier shall provide CVs of their key personnel (Supervisors and above) for agreement by contractors, along with a 20% sample of experience sheets for security guards being employed at the site. The 20% sample shall be chosen at random by the Contractor who reserves the right to request that any member of the security staff, who does not have adequate experience is replaced with another member of staff who does have the required experience.

6.2. SECURITY PERSONNEL – CODE OF CONDUCT

6.2.1. It is vital that all security personnel conduct themselves in a manner that does not reflect negatively on either the Security Supplier, Contractor or Rogun JSC. To ensure this, all security personnel shall comply with the following minimum standards.

Acceptable Conduct

All security personnel shall:

- Always conduct themselves in a professional and courteous manner.
- Be firm, calm, and courteous in dealing with all people and enforcing the required security actions. The Contractor is to ensure their staff are also compliant, courteous, and respectful in their dealings with the Security Supplier's staff.
- Be smartly dressed in the supplied uniform for the duration of their shift. (See also the next sub-section)
- Be punctual for their shift, leaving sufficient time to be at their allocated post on time, with the right equipment and correctly dressed.

It is not acceptable to:

- Smoke whilst on duty, and no smoking should be undertaken in vehicles.
- To use a personal mobile phone whilst on duty.
- To misuse/make unnecessary or private phone calls whilst on duty.
- To sleep whilst on duty.
- To allow personal relationships to influence professional behaviour.
- To allow a group or individual to bring undue influence or pressure to bear on security operations. If in doubt, apply the taught security procedures, the Contractor shall support reasonable behaviour.
- Possess drugs, alcohol or illegal substances whilst on duty. This will result in dismissal.
- Engage in any other commercial activity, of any kind, whilst on duty. This applies to also being on-site whether on duty or not, unless authorised by the relevant department of the contractor.

In addition, the following should be adhered to:

- Food should only be consumed during scheduled break periods. Special arrangements during Ramadan shall be put in place.
- Maintaining confidentiality of site information, activities, personnel, and security procedures at all times.

Acceptable Behavioural Standards

Acceptable behaviour should be enforced for both the accommodation camps and worksites. Suggested behavioural standards for all staff are included at **Appendix J.**

Uniform and Standards of Dress

All security personnel shall be smartly dressed with appropriate levels of cleanliness as follows:

- Uniform has been washed and pressed.
- Boots have been cleaned. (The wearing of sandals or non-protective footwear should be reported as a safety Near-Miss.)
- Any damage to the uniform has been competently repaired or the article replaced.
- Maintaining a good standard of personnel cleanliness, including washing, neat hair and facial hair.

Standard Equipment

All security personnel shall be issued with the following equipment to support the delivery of their daily assigned activities:

1) Serviceable and suitable uniforms x No. 3 per man (minimum).
2) Cold and wet weather clothing.

3) Hi-visibility vest – to be used where required based on task safety risk assessment.
4) Suitable boots.
5) Gloves suitable to their tasking, examples being:
   a) Vehicle searching – protective gloves from dirt etc.
   b) People or luggage searching – clean tactile gloves.
   c) As a minimum any mobile patrol should carry at least one pair of disposable gloves per person.
6) Notebooks and pens.
7) A fully charged flashlight.
8) The required radio or mobile communications device. This should be fully charged, and the user should understand the re-charging requirements.
9) Whistle for attracting attention.

6.2.2. The Security Supplier shall ensure that all equipment is maintained in a clean and serviceable condition.

6.2.3. Any unserviceable, damaged or lost equipment should be reported as soon as practicable to the relevant supervisor or manager so that replacement equipment can be issued. It is not acceptable for a shift member to not have the serviceable standard equipment and therefore the shift supervisor should have access to spare items for immediate replacements.

6.2.4. All security personnel should undertake familiarisation and safe use training on equipment. Where the equipment is only used periodically, or common mistakes dictate, refresher training should be provided.

6.2.5. All security staff should wear the appropriate PPE for the task being undertaken. Tasks should be risk assessed by the Security Supplier and the relevant safety actions taken. Unsafe practices or the lack of an adequate safety risk assessment shall not be tolerated.

Standard Information

6.2.6. It is essential that each member of security staff carries a minimum ‘Reference Aide Memoire’ of vital information for the site they are employed upon. This should include the relevant security and emergency/incident management information referenced in this document and the SSP and Site Security Instructions (SSI). However, the security staff is also on site to aid the efficient operation of the site. To help achieve this, it is required that security staff include in the aide memoire general site information. This information should consist of, but not be limited to:

Maps/diagrams showing:

1) The site layout with any sensitive area information removed.
2) Parking areas.
3) Pedestrian movement routes to help explain how to reach certain locations.
4) Locations of facilities, such as toilets or first aid points.
5) Defibrillator unit locations.

6.2.7. Maps/diagrams should contain simple annotation in the common languages spoken by regular users of the site. At a minimum, this should be in Tajik and English.

6.2.8. Opening and closing times if applicable.

6.2.9. The prohibited item list in a pictogram form.

6.2.10. Emergency procedures and relevant information such as muster points etc.

6.2.11. Standard notebook event recording formats of the information that shall be required to be entered into the daily security log.

6.2.12. Blacklist or Watchlist details for individuals or vehicles.

6.2.13. Complaints forms to issue to site users if requested, and details of where these should be deposited.

Security Vehicles

6.2.14. The Security Supplier should ensure that security vehicles comply with the following:

- Wherever security personnel are present at a site, they shall require access to a security vehicle. The number of vehicles should be scaled to the number of security personnel, the number of static tasks and mobile tasks.
- As specified in site scope of works and suitable for the site.
- Clearly marked as security vehicles on the front, both sides and rear. Any lettering should be readable from a minimum distance of 20.0m.
- Correctly registered, have proof of insurance and maintenance record.
- Contain not less than half a tank of fuel at any point in time.
- 4x4 SUV, 2018 or newer models.

Each vehicle should carry the following minimum equipment:

1) Comprehensive emergency first aid kit (x 1).
2) Emergency flashlight (x 1).
3) Fire extinguishers (x 2).
4) Fire Blanket (x 1), suitable for use on a person.
5) Jumper cable, for starting other vehicles (x 1).
6) Light bar (orange colour).
7) Recovery strap (x 1).
8) Sand shovel (x 1).
9) Small traffic cones (x 4).
10) A roll of warning tape, minimum 25.0m.
11) Traffic control wand (stop / go) – battery operated (x 2).
12) Vehicle mounted radio communications.
13) Vehicle tire changing equipment and spare wheel.
14) Portable air pump for the tires.
15) 10 Litres of potable drinking water in sealed bottles for emergency use.

6.2.15. Drivers should perform vehicle checks before using a vehicle daily. The Security Supplier is to prepare the 1st Parade Check List and ensure drivers shall be suitably trained and follow the requirements.

6.2.16. All drivers should hold a valid Tajikistan driving licence and be adequately covered by the Security Supplier's insurance. Drivers should also be familiar with the vehicle they have been asked to drive and it is the SUPPLIER's responsibility to ensure safe driving practices are enforced.

6.2.17. Security vehicles should never be used for personal use.

6.3. USE OF FORCE

6.3.1. In accordance with IFC Performance Standards and the World Bank ESF, the Rogun HPP project is committed to ensuring that any use of force by private security is lawful, proportional, and fully aligned with international standards. Recognizing that the project site has a porous perimeter, with nearby villagers occasionally crossing into the area with livestock, the following use-of-force guidelines have been established to maintain security while respecting local communities and people's rights.

Principles of Use of Force

- Private security personnel should be authorized to use force only as a preventive or defensive measure, and solely when necessary to protect people, project assets, or prevent an imminent threat.
- Any force used should be proportional to the immediate nature and level of threat posed, ensuring the minimum force necessary to defuse the situation is applied.
- Non-lethal and non-aggressive means of deterrence are prioritized, with a focus on de-escalation and communication, especially in cases where villagers and livestock may inadvertently enter the project area.

Training

- All security personnel including military shall undergo rigorous training on the appropriate and controlled use of force, conflict de-escalation techniques, and respectful treatment of people in alignment with IFC and World Bank ESF standards. This training emphasizes understanding and sensitivity towards the local community, including those awaiting relocation.
- Training includes modules on international laws and standards, ensuring personnel understand and respect the rights of all individuals, including local villagers and community members who may be present near or within project boundaries.

Specific Considerations for Local Communities

- In recognition of the nearby villagers who may cross the site boundary with livestock, security personnel are trained to first engage in clear, respectful communication before considering any action.
- Private security should take special care to avoid any actions that could be perceived as harassment or intimidation, particularly towards women, children, or other vulnerable groups within the local community.

Accountability and Monitoring

- All incidents where force is used should be thoroughly documented, reported, and reviewed by Rogun JSC, to ensure compliance with established policies and alignment with IFC and World Bank ESF guidelines.
- Regular audits and performance reviews shall be conducted to evaluate compliance with the use-of-force policy, with feedback incorporated to enhance the effectiveness of security practices and reinforce the focus on people's rights and proportionality.

Commitment to Resettlement Process

- Security personnel are instructed to respect the presence of villagers who remain on or near the project site due to the ongoing resettlement process. Security actions are designed to

avoid interference with or disruption to community resettlement activities.

6.4. COMMUNITY ENGAGEMENT AND GRIEVANCE MECHANISM

6.4.1. In alignment with IFC Performance Standards and World Bank ESF guidelines, Rogun JSC recognizes the importance of engaging with the community to ensure that security measures are implemented in a manner respectful of people and sensitive to community concerns. To this end, Rogun JSC shall establish robust mechanisms for community engagement and grievance redressal, fostering trust and mitigating risks associated with security arrangements.

Community Engagement

6.4.2. Rogun JSC is engaging with community members on matters related to security. These efforts are being undertaken in coordination with the Community Relations team to ensure a collaborative and inclusive approach. Specific measures include:

Information Sharing: Regular communication with community members to provide transparent information about project security arrangements and protocols while safeguarding sensitive security details.

Consultation Forums: Organizing community consultations, meetings, and workshops to solicit feedback, address concerns, and create a platform for dialogue on security-related issues.

Community Feedback Integration: Incorporating community feedback into security management practices, especially when it pertains to the behaviour of security personnel or the impact of security measures on daily life.

Dedicated Liaison Officers: Appointing community liaison officers to act as a bridge between the project and the local population, ensuring continuous dialogue and timely issue resolution.

6.4.3. These efforts are aimed at building mutual understanding, enhance the project's social license to operate, and minimize potential conflicts or misunderstandings.

Grievance Mechanism

6.4.4. To address community concerns effectively, PMG and Rogun JSC are implementing a formal grievance mechanism aligned with World Bank ESF requirements. The mechanism enables community members to voice complaints or raise concerns related to security personnel or measures impacting their well-being. Key features include:

- **Accessibility and Transparency:** The grievance mechanism is easily accessible to all community members, with clear procedures for lodging complaints, whether in person, online, or through designated liaison officers.
- **Timely Response:** Complaints are acknowledged promptly, investigated thoroughly, and resolved within specified timeframes to ensure accountability and responsiveness.
- **Monitoring and Reporting:** All grievances are logged and tracked, with regular reporting to analyse patterns, address systemic issues, and ensure continuous improvement.
- **Risk Mitigation:** Rogun JSC is adopting measures to mitigate risks associated with security arrangements, such as:
    - Regulating guard behaviour both on and off-site to prevent misconduct.
    - Establishing protocols for coordination with public security forces to ensure appropriate responses to demonstrations, civil disorder, or criminal activity.

- Providing communities with non-sensitive information about security measures to address concerns without compromising overall safety.

This grievance mechanism includes principles of confidentiality, non-retaliation, and respect for people, ensuring that all complaints are handled fairly and transparently.

6.5. ASSESSING ALLEGATIONS OR INCIDENTS RELATED TO SECURITY PERSONNEL

6.5.1. In line with IFC Performance Standards and World Bank ESF guidelines, Rogun JSC is committed to upholding high standards in managing allegations and incidents related to security personnel conduct. To ensure that incidents are addressed professionally and impartially, Rogun JSC is establishing policies and procedures for evaluating security-related incidents and allegations. These apply to security personnel operating on the project site, as well as to any off-site events that involve security forces associated with the project.

6.5.2. **Core Considerations for Assessing Security-Related Allegations or Incidents**

- Rogun JSC is aligning the scope and level of response to the severity and credibility of the allegation or incident.
- Rogun JSC is implementing policies for receiving, assessing, documenting, and investigating security-related allegations, with protocols covering documentation, confidentiality, inquiries, reporting, corrective actions, monitoring, and communication.
- Allegations involving unlawful or abusive acts by security personnel are reported to appropriate authorities as required, with careful judgment exercised in instances where concerns exist regarding the treatment of individuals in custody.

Key Steps in the Process

Record the Allegation or Incident

6.5.3. All security-related allegations and incidents, regardless of severity, are recorded through a formal mechanism, whether reported via an incident report, grievance mechanism, or any other means of communication. Severe incidents are reported promptly to senior management, and any potentially criminal wrongdoing is escalated to relevant authorities.

Prompt Information Collection

6.5.4. Information is gathered immediately following an incident, detailing the context, individuals involved, timing, location, and other relevant circumstances. Where appropriate, statements or photographic evidence may also be obtained.

Confidentiality Protections

6.5.5. Rogun JSC is committed to ensuring confidentiality to protect alleged victims, witnesses, and complainants. Confidentiality protocols may include using anonymous identifiers and informing parties of how their identity shall be managed. Sensitive data is handled with strict confidentiality throughout the assessment process.

Incident Assessment and Inquiry

6.5.6. Each allegation or incident is reviewed against security policies to determine whether noncompliance or misconduct occurred. For serious allegations, such as excessive use of force, injury, or unlawful acts, a comprehensive inquiry is conducted. Criminal acts are referred to authorities.

Documentation

6.5.7. The assessment process is documented thoroughly, detailing sources of information, evidence, analysis, and findings. If evidence is limited, this is noted, and efforts are made to obtain any missing information. Reports should be fact-based and impartial, with all documentation securely classified as confidential.

Reporting Unlawful Acts

6.5.8. Any criminal or unlawful acts by security personnel is reported to the appropriate authorities, balancing the need for transparency with the requirement to ensure humane treatment of those involved. Rogun JSC cooperates with government-led investigations, ensuring internal assessments do not interfere with official processes.

Corrective Actions

6.5.9. Rogun JSC is implementing corrective actions to prevent recurrence of incidents, including disciplinary actions when security personnel deviate from policies. This approach allows for continual improvement in security practices, addressing any lessons learned from incidents through updates to company policies.

Monitoring and Communication

6.5.10. Rogun JSC is monitoring ongoing investigations and communicate outcomes to relevant parties, protecting confidentiality and the rights of victims. Where appropriate, Rogun JSC shares any lessons learned and resulting policy improvements with relevant stakeholders to enhance transparency and maintain trust.

7. APPENDICES

APPENDIX A – GUIDANCE FOR PREPARING THE SECURITY THREAT RISK ASSESSMENT (STRA)

Project Context

7.1.1. The Rogun Hydroelectric Power Plant (HPP) is a significant infrastructure project in Tajikistan, featuring the highest dam in the world at 335 meters. This project, initiated in the 1960s, aims to harness the hydropower potential of the Vakhsh River. The Rogun HPP is designed to have six turbines with a combined capacity of 3780 MW, expected to generate 13 to 17 billion kWh of electricity annually upon completion. The primary purpose of the Rogun HPP is to address Tajikistan's critical winter electricity shortages and meet future energy demands, while also respecting the water needs of downstream riparian countries.

7.1.2. The construction of the Rogun HPP has faced several interruptions since it began in 1980, primarily due to the breakup of the Soviet Union and the need for comprehensive technical, economic, and environmental studies. After resuming in 2008 and pausing again, construction recommenced in 2015. The project is expected to be completed by 2032, with the dam reaching its full height and the reservoir gradually filling up over the following years, reaching maximum water levels by 2039.

7.1.3. The powerhouse and related infrastructure are located in caverns that require further excavation to address deformation and other issues caused by floods and geological conditions. Additional works include the construction of diversion tunnels and spillways to manage normal flows and floodwaters, multi-level intakes, access tunnels, and temporary structures to handle river flows during construction. Excavated spoil is stored and reused in dam construction wherever possible.

7.1.4. Beyond electricity generation, the Rogun HPP offers several other significant benefits. It provides downstream flow regulation, helping to mitigate shortages in dry years, and enables electricity production for export to neighbouring countries such as Pakistan and Afghanistan. The project also enhances flood routing capacity, protecting the existing Vakhsh cascade, including the Nurek dam, from the Probable Maximum Flood. Additionally, by retaining high sediment loads, Rogun will extend the operational life of the Nurek reservoir and the Vakhsh cascade by over 100 years.

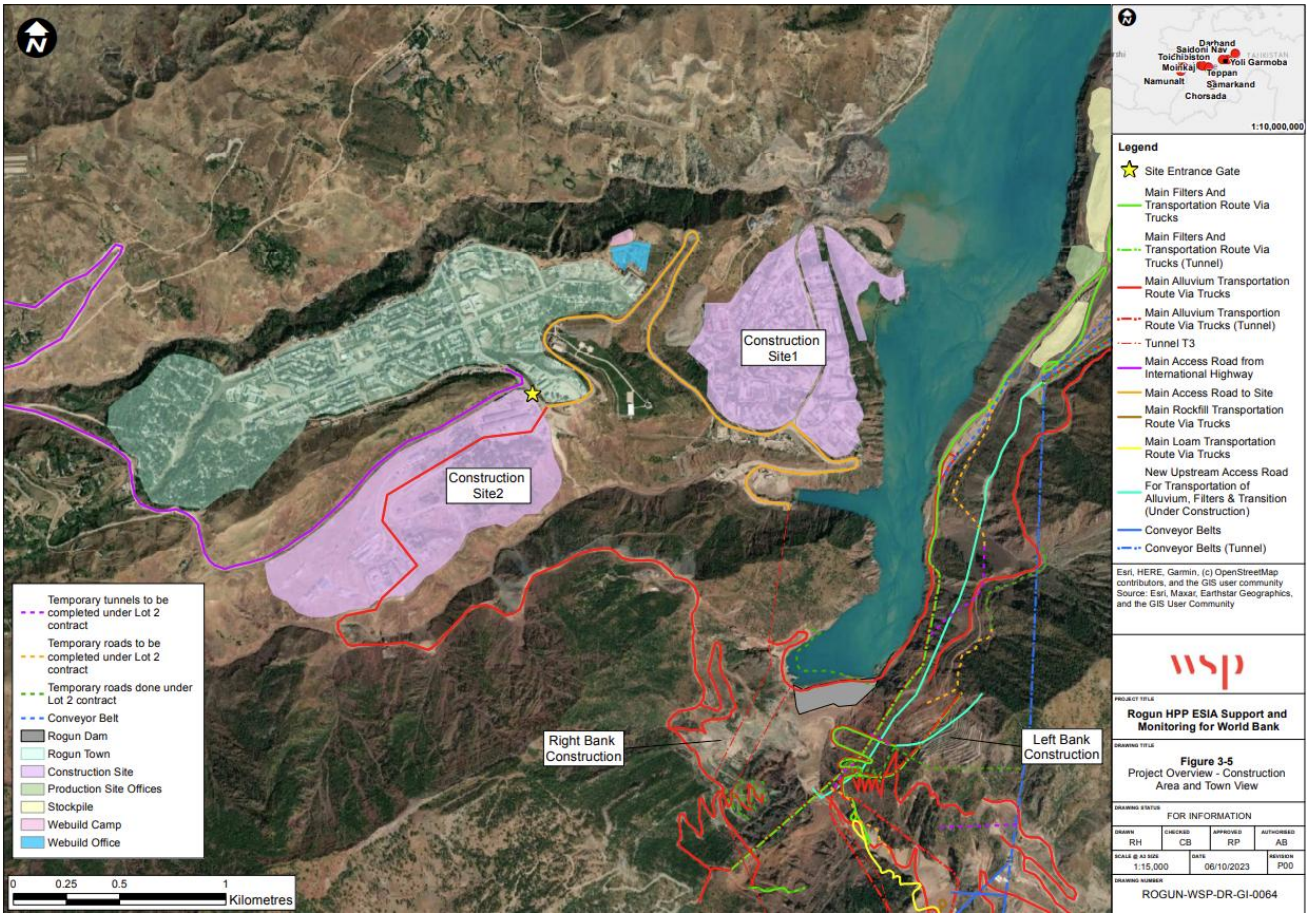


Figure A-1 - Rogun HPP project site

Asset Criticality Analysis

7.1.5. The asset criticality assessment for the Rogun Hydroelectric Power Plant (HPP) underscores the importance of all physical assets to the project's success. However, the most critical assets include the dam structure, which holds back the water, the two operational turbines generating electricity, the four turbines under construction, and the powerhouse housing the turbines and generators. The Rogun HPP, a hydroelectric power project, features assets distributed across the site, including the dam structure, operational and under-construction turbines, powerhouse, generators, spillways, intake structures, penstocks, control systems, switchyard/substation, diversion tunnels, access roads and tunnels, reservoir, sediment management systems, safety and monitoring equipment, construction equipment and materials, and the workers' camp area. These assets are strategically spread out to maximize the natural geography, creating critical national infrastructure locations. Overall, the Rogun HPP site and its assets should be considered a single critical asset, with each component playing a vital role in the project's overall functionality and success.

7.1.6. It should be noted that most critical assets are the people themselves living near the Rogun HPP dam site. These can be different user groups The following security analysis will consider the threats' consequences on the people and security management plan will be designed to protect the residents, workers and visitors.

7.1.7. Given this specific project context, the standard methodology of asset criticality has not been used. However, the following table provides a summary of the primary assets, their value, and their

contribution to the project as a whole. This will be used to identify areas for protection as part of the developing security strategy:

Table A-1 Asset Criticality Table

Asset	Rating	Asset Criticality/Importance
Rock-fill Dam Structure	Very High	The main body of the dam, which holds back the water, is the most critical asset. It ensures the stability and functionality of the entire project.
Operational Turbines	Very High	The two turbines that are currently generating electricity are essential for the immediate production of power, contributing to the project's primary goal
Turbines (Under Construction)	Very High	The four turbines that are still being installed are crucial for future capacity and efficiency. Their completion will significantly enhance the plant's output
Powerhouse	Very High	The building or cavern housing the turbines and generators is vital for protecting and maintaining the operational integrity of the power generation equipment.
Generators	Very High	Machinery connected to the turbines that convert mechanical energy into electrical energy are essential for electricity production.
Spillways	High	Structures that allow excess water to bypass the dam to prevent overflow and maintain safe water levels are critical for managing water flow and preventing structural damage
Sluice Gates	Very High	A movable barrier that controls the flow of water through a dam
Intake Structures	High	Facilities that control the flow of water into the turbines are necessary for regulating water input and ensuring efficient turbine operation.
Penstocks	High	Large pipes that carry water from the Valve house to the turbines are essential for directing water flow to the turbines
Control Systems	High	Equipment and software used to monitor and control the dam's operations, including turbine performance and water levels, are crucial for operational efficiency and safety.

Asset	Rating	Asset Criticality/Importance
Switchyard/Substation	High	Facilities where the generated electricity is transformed and distributed to the power grid are essential for integrating the power plant with the electrical grid
Access Roads and Tunnels	High	Infrastructure that provides access to the dam and powerhouse for construction and maintenance is necessary for logistical support and operational maintenance.
Surge Chamber	High	This controls pressure fluctuations in the penstock to prevent damage from water hammer effects.
Draft Tube	Medium	This conveys water from the turbine outlet to the tailrace, ensuring efficient water flow
Tailrace	Medium	These channels the water back into the river or stream after it has passed through the turbines.
Valve House	High	A structure that houses various valves and control mechanisms to control the flow of the water from reservoir to turbines
Pressure Tunnel	Very High	A pipe structure that conveys water from the reservoir to the Valve house under high pressure
Transformer	High	An electrical system to that steps up the voltage of the electricity generated by the turbines
Residential Areas	Medium	A residential space built to accommodate the staff; workers involved in the dam construction.
Quarry	Medium	A site located within the Rogun dam area for the extraction of rocks which will be used for dam construction.
Security Post	Medium	Located at the road to dam site to control the vehicle access and inspection
Storage Facility/Warehouse	Medium	Onsite storage facilities built to store the construction equipment and material securely.

Threat Assessment

7.1.8. The aim of the threat assessment is to clearly identify the range of potential threats arising from the external and internal security environments, and their relevance to the development. The threat assessment is concerned with identifying those events, aggressors, or adversaries that can cause

losses to the development, organization, or individual assets. Threats are defined as deliberate actions intended to cause injury or death to people within Rogun HPP Dam project or damage or loss of critical assets. For dam projects, these actions fall into the following categories:

- National Level
- Political and social instability
- Crime / Organized Crime
- Terrorism
- Sabotage

7.1.9. International threats, which are based on the notion of an attacker or adversary, include an assessment of the intent and capability of an individual or group to undertake actions that will result in harm or the expectation of harm to another individual, group, organization, or community. This analysis includes:

- Identifying the range of potential threats to an individual, organization, or community.
- Identifying the intent and capability of the identified group or individual to carry out an attack.
- Examining the possible ways in which these threats may interact with the critical asset, either directly or indirectly, and understanding the specific impacts that could arise.
- Determining how likely these threats are to occur within a defined time frame or locality.

7.1.10. If possible, the threat assessment should culminate in the development of a range of credible threat scenarios or Design Basis Threats (DBTs). These express more specifically how the threat is likely to manifest. For example, while assessments may identify a general threat from terrorism, it is more helpful, particularly in the planning and design process, for a range of DBTs to be considered, such as a Vehicle Borne Improvised Explosive Device (VBIED), a Person Borne Improvised Explosive Device (PBIED), or a coordinated Marauding Terrorist Attack (MTA). This helps project teams to better understand how the threat may apply to the development and what the vulnerabilities are; this in turn can be used to inform a more specific treatment plan. These scenarios should be based on historical trend data, previous incidents, intelligence (from local police crime advice/intelligence), and open-source material. These are shown as case studies for each of the primary DBTs.

Threat Rating and Definition

7.1.11. The threat ratings and descriptions to be applied for a STRA are provided in following table. Threat ratings are a combination of the assessed capabilities and intentions of the threat actors. There is a degree of subjectivity in the rating process, which relates to either insufficient data being available or the lack of a comprehensive threat history. The rating for the threats is based on the likelihood of that threat to manifest in general based upon motivations, i.e., not specifically related to an asset but generally to the heritage sector. As threats change, ratings should be modified.

Table A-2 Threat Table

THREAT	INTENT	CAPABILITY
Very High	Communicated in public, organized, and detailed decision to commit the threat act.	Resources are available locally. Requires unskilled personnel.
High	Communicated in public, committed but unorganized intention to commit the threat act.	Resources are available within the region. Requires unskilled personnel.
Medium	Displayed intention to commit the act when presented with an opportunity.	Resources are available within the region. Requires skilled personnel.
Low	The overall intent to commit the act is low.	Limited availability of resources within region. Requires highly skilled personnel.
Very Low	There is no information to support any intent.	Resources and skills are extremely controlled and limited.

Critical National Infrastructure

7.1.12. The UK government and National Protective Security Authority (NPSA) (formally CPNI) have set definitions of what is classified as CNI. The UK government's official definition of CNI is:

7.1.13. "Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state."

7.1.14. According to the CPNI website, the definition of CNI is:

7.1.15. "National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example)."

7.1.16. In the UK, there are 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport, and Water. Several sectors have defined 'sub-sectors'; Emergency Services for example can be split

into Police, Ambulance, Fire Services and Coast Guard. However, it should be noted that not everything within a national infrastructure sector is judged to be 'critical'.

7.1.17. Rogun Hydropower Plant is considered critical national infrastructure due to its pivotal role in the country's energy security and economic development. The Rogun Dam, once completed, is expected to be the tallest in the world, significantly boosting Tajikistan's capacity for electricity generation and reducing its reliance on energy imports. This project is not only vital for meeting the domestic energy needs of a country that frequently experiences power shortages but also for enabling Tajikistan to export electricity to neighbouring countries, thereby enhancing regional energy cooperation and economic stability. Additionally, the dam is a national symbol of progress and self-sufficiency, contributing to the country's efforts in nation-building.

Vulnerability Assessment

7.1.18. The Rogun HPP project, despite benefiting from a multi-layered security setup, faces certain vulnerabilities due to its location, profile, and current security arrangements. While the involvement of the national military, police, and private security, along with the natural topography, provides some deterrence, detection, and response capabilities, there are critical gaps that leave the site susceptible to terrorism and criminal activities. The most notable vulnerabilities include:

- **Porous Perimeter:** The project is surrounded by hills, making the perimeter difficult to secure completely. This natural terrain creates unmonitored and accessible entry points.
- **Villagers within the Project Site:** Some villagers still reside within the project site as part of an ongoing rehabilitation process, posing potential security and operational risks.
- **Undefined Pedestrian Access Points:** Pedestrians currently use vehicle access control points due to the absence of designated pedestrian access areas, and inadequate screening enhance MTA, PBIED risks.
- **Unsecured Tunnel Entrances:** Tunnel entrances lack access controls or physical barriers, leaving critical infrastructure exposed to unauthorized entry or sabotage.
- **Inadequate Access Controls to Power Generation Room:** The power generation room, accessible through a tunnel, does not have proper vehicle or pedestrian access controls, creating a significant vulnerability.
- **Disconnected Security Systems:** The centralized command room is not integrated with the site security control rooms, reducing the efficiency of security monitoring and response coordination.
- **Inadequate Perimeter Fencing:** Construction areas lack adequate perimeter fencing, leaving these zones vulnerable to unauthorized access.
- **Limited Screening Measures:** Vehicle and pedestrian screening measures at access points are insufficient to detect and deter potential threats effectively.
- **Hostile Vehicle Mitigation (HVM):** While deployable HVM measures are in place, they are not crash-rated. Vehicle entrances are not designed to deny or withstand hostile vehicle attacks, leaving critical access points vulnerable.

Risk Analysis

7.1.19. Risk analysis should provide decision makers with sufficient information to make an informed decision on the need for increasing or decreasing the investment for protection across the spectrum of assets under consideration. The risk analysis involves the consideration of the risk description, developed in the previous identification step, along with the combined outputs of those analyses (threat, criticality, and vulnerability analyses) that contributed to its formulation. The risk analysis should examine how these factors interact to determine an overall level of risk through a consideration of the consequences of the event occurring combined with the likelihood of the event with that consequence. These risks should be prioritised so that project teams can readily identify which risks require the greatest level of consideration during preparation of the security risk management plan.

7.1.20. Risk analysis requires a careful consideration of both likelihood and consequence. The likelihood refers to the chance or probability of an incident or event. The likelihood can be estimated as an absolute probability (e.g. occurring with a probability of between 0 and 1), as a percentage chance of occurrence, as the chance that something will occur over a defined period (e.g. 'over the next two years') or as a general statement of likelihood (e.g. certain, unlikely). The consequence of safety and security risks can usually be expressed as a measure of financial loss, stakeholder/community impact, reputational damage, loss of operational capability, or health and safety implications. Impacts derived as part of the criticality assessment are used to inform the determination of overall risk consequence.

Table A-4 Likelihood Rating Table

Rating	Likelihood
Almost Certain	Is expected to occur in most circumstances. Has occurred on a frequent basis in similar organisations and /or locations and almost certain to occur during the life cycle of the property/facility/premises.
Likely	Will probably occurs in most circumstances. Has occurred often in similar organisations and /or locations and it is likely to occur during the life cycle of the property/facility/premises.
Possible	Could occur at some time. Has occurred occasionally in similar organisations and /or locations and it is possible that it will occur during the life cycle of the property/facility/premises
Unlikely	May occur in exceptional circumstances. Has seldom occurred in other similar organisations and /or locations and but is unlikely to occur during the life cycle of the property/facility/premises.
Rare	Expected to not occur. It's never occurred in the history of a similar organisation and /or locations and is not expected to occur in the life cycle of the property/facility/premises.

Table A-5 Consequences Rating Table

	Life and Health	Reputation	Property & Equipment	Operations
Severe	Multiple fatalities	Loss of global reputation. Sustained national/global media scrutiny.	Asset damage/Loss of more than 50%	Critical failure of performance and productivity. The impact threatens the organisation and/or survival of the project.
Major	Single fatality and multiple critical Injuries	Loss of regional reputation. Long term reputation impact.	Asset damage/Loss of 20-50%	Breakdown of key operations leading to reduced performance and productivity. Survival of the project/activity/organisation is threatened.

	Life and Health	Reputation	Property & Equipment	Operations
Moderate	Multiple serious injuries requiring hospitalisation.	Loss of local reputation and persistent national concern. Long term brand and reputation impact	Asset damage/Loss of 5-19%	Permanent change to operations. Impact on the organisation resulting in reduced performance and productivity. Organisations existence is not threatened but a review is required.
Minor	Multiple minor injuries or single serious injury.	Temporary local brand and reputation impact	Damage/Loss of less than 5%	Minor delay requiring temporary change to operations but is dealt with at an operational level.
Limited	Minor injury or first aid treatment.	Local concerns, quickly forgotten. Brand and reputation unaffected.	Immediately repairable. Minor damage.	No noticeable delay or operational impact

APPENDIX B -SITE SECURITY PLAN (MINIMUM CONTENTS)

(To be Filled by the Contractor and Approved by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	

The following detail is the mandatory minimum requirement for the Contractors SSP. It is expected that additional site-specific sections will need to be added.

This approved document should be submitted to Rogun JSC, a minimum of 4 weeks prior to any work starting on the construction site.

This is an auditable document.

1.	**Introduction**
a.	**Scope of the document**
b.	**Locations covered by this SSP**
c.	**Phasing Programme and identified changes in security needs.**
d.	**Audit Timetable and Record.**

2.	**Organisation**
a.	**Security Organisation.**
b.	**Roles and Responsibilities.**
c.	**Contact Details.**

3.	**Security Risk Assessment**
a.	**Reference to the STRA document.**
b.	**Summary of the STRA outcomes.**
c.	**Audit Timetable.**

4.	**Concept Of Security Operations**
a.	**Detailed explanation of how security will operate at the site.**
b.	**Technical Security Measures.**
	i. **Fences, Gates.** ii. **Vehicle Barriers, if deployed.** iii. **Intruder Detection.** iv. **Surveillance Systems.** v. **Access Control Systems.** vi. **Locks and Windows**
c.	**Operational Security Measures.**
	i. **Security Static Locations.** ii. **Security Patrols.** iii. **Access Control Points – vehicles and pedestrian.** iv. **Security Checks and Routines.**

d.	**Procedural Security Measures.**
i.	**Identity Cards.**
ii.	**Site Entry Procedures.**
iii.	**Control Room Procedures.**
iv.	**Contingency Procedures.**

5.	**Security Infrastructure Design**
a.	**Layout of Security Infrastructure at the site.**
b.	**Performance Requirements for Security Infrastructure.**
c.	**Security Systems Integration Plan.**

6.	**Site Security Instructions**
a.	**Production Responsibility.**
b.	**Audit Timetable.**

7.	**Emergency Response Plan**
a.	**Reference to the Rogun JSC and contractors ERP.**
b.	**Audit Timetable.**

APPENDIX C - SSP COMPLIANCE CHECKLIST

(To be Filled by the Contractor)

Contractor:	
Rogun JSC:	
City/Site/Location:	

The contractor should use this SSP Compliance Checklist to check they have adequately fulfilled their duties to Rogun JSC around the provision of site security management.

#	Action Required	Status
1	*Example: Receive Threat Briefing from Rogun JSC*	*Complete 02/12/24*
1	Receive the Rogun JSC Threat Briefing	
2	Complete the draft of the STRA for the site	
3	Has Rogun JSC approval of the STRA been received?	
4	Complete the draft of the SSP for the site	
5	Has Rogun JSC approval for the SSP been received?	
6	Draft the SSP audit timetable and submit to Rogun JSC	
7	Assign roles and responsibilities to named individuals and record their acceptance of this	
8	Install security infrastructure as per Security Management Standard with any agreed enhancements required	
9	Install the SCR	
10	Training and Awareness required to staff	
11	Draft ERP created with reference to Rogun JSC ERP	
12	Has ERP approval from Rogun JSC been received?	

APPENDIX D - SUPPLIER SITE SECURITY INSTRUCTIONS (SSI)

(To be Filled by the Contractor and Approved by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	

The following detail is the mandatory minimum requirement for the SUPPLIER SSI.

This approved document should be submitted to Rogun JSC, a minimum of 2 weeks prior to any work starting on the construction site.

This is an auditable document.

8. Introduction
e. **Scope of the document.**
f. **Purpose and Intent of the Document and how it should be used.**
g. **SUPPLIER Headquarters Contact Details.**
h. **Organogram of Management Structure.**

9. Applicable Sites
d. **Statement of all sites covered under the SSI.**
e. **Appended Site Layouts showing key security locations.**

10. Key Standards and Compliance
d. **Matrix showing the standards and regulations that will be complied with. To include key Rogun JSC and Contractors Standards and management Plans:**
vii. Security Management Plan. **viii. SSP.** **ix. ERP**
e. **Linkage to Rogun JSC Information Security Policy.**
f. **Linkages to Other Processes, Policies and Procedures (Health & Safety, Quality, Environment).**
g. **Linkages to Government Regulations.**

11. Roles and Responsibilities
e. **Full Organogram of Security Structure on each Applicable Site.**
i. **To include a standard Security Team Structure from Supervisor to Security Guards.**
f. **Role of Security Staff by Job Title.**
g. **Code of Conduct.**
h. **Staffing and Rostered Positions.**

12. Communication and Consultation
a. **General.**

b.	**Liaison and Interaction with Government Departments.**
c.	**Incident and Hazard Reporting and Analysis.**
d.	**Responding to Security Directions given by Rogun JSC.**
e.	**Training and Awareness.**
f.	**Security Exercises and Drills.**

13. Reviews, Audits and Inspections	
a.	**Security Reviews.**
b.	**Inspections and Audits.**
c.	**Rogun JSC audits need to be identified against a timetable.**
d.	**Client meetings.**
e.	**Monthly Management Reports to client.**

14. Assignment Instructions	
a.	**Introduction to AI purpose.**
b.	**Standard Format.**
c.	**Review and Audit of AIs.**
d.	**List of AIs included in the Appendices.**

Site Plans	
Appendices Covering Each Assignment Instruction	
Should be prepared to cover the security tasks, activities and actions the Security Staff do to provide a secure site, including reporting, administration etc. The following is the minimum list of AIs to be produced, and it is expected that the Security Supplier as a competent provider will amend and add to the AIs as suitable for their role. **The AI should content the level of detail which allows the relevant person to perform their duties without ambiguity.**	
Assignment Instructions	
a.	**Security Control Room: Camera Operator Duties.**
b.	**Security Control Room: Supervisor Duties.**
c.	**Security Control Room: Access Control System Enrolment.**
d.	**Security Control Room: Incident Management Duties.**
e.	**Threat Level Security Requirements – Base, Enhanced and Severe.**
f.	**Basic Guarding Duties.**
g.	**Guard Supervisory Duties.**
h.	**Mobile Patrol Duties.**
i.	**Guard Tour System Usage.**

j. **Lockable Building Checks.**
k. **Perimeter Security Checks and Damage Reporting.**
l. **Perimeter Intrusion Immediate Actions Procedure.**
m. **Vehicle Access Control Point Duties.**
n. **Vehicle Manual Searches.**
o. **Vehicle Access Control Point Logging and Reporting.**
p. **Vehicle Passes Issuing Procedure.**
q. **Parking Enforcement Procedures.**
r. **Pedestrian Access Control Point Duties.**
s. **Personnel and Baggage Searching.**
t. **Pedestrian Access Control Point Logging and Reporting.**
u. **Visitor and Guest Procedures.**
v. **Return of Visitor Passes and their Destruction.**
w. **Visitor and Guest Escort Requirements.**
x. **Visitor and Guest PPE Requirements.**
y. **Staff Entry Requirements.**
z. **Photography Permit Procedure.**
aa. **Site Delivery System Checks.**
bb. **Delivery Escorts.**
cc. **Delivery of Mail and its Security.**
dd. **Response to Suspect Packages or Mail.**
ee. **Key Management and Issuing Procedure.**
ff. **Traffic Offences and Issuing of Warnings.**
gg. **Reporting.**
• **Daily.** • **Weekly.** • **Monthly.** • **Exception.**
hh. **Identity and Access Credential Management Procedures.**
ii. **Temporary Parking Permits.**
jj. **Evacuation and Procedures.**
kk. **Fault Reporting Procedures.**
ll. **Traffic Control Duties.**
mm.**Site Emergency Procedures.**
nn. **Maintenance and Care of Security Equipment.**
oo. **Severe Weather Duties.**
pp. **Site Materials Removal Recording Duties.**
qq. **Effective use of the Security Radio Network.**
rr. **Emergency Contact and Call Out Information.**

ss. **Prohibited Items Procedures.**
tt. **First Aid Duties and Medical Assistance.**
uu. **Fire Fighting Duties.**
vv. **Use of Force and Self Defense Techniques.**
ww. **Police and fire liaison.**
xx. **Lost Property Procedures.**

APPENDIX E -SSI COMPLIANCE CHECKLIST

(To be Filled by the Contractor and Reviewed by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	

The SUPPLIER should use this SSI Compliance Checklist to check they have adequately fulfilled their duties to the CONTRACTOR in the delivery of site security.

#	Action Required	Status
1	*Example: Security Staff familiar with SSI Document.*	*Complete 02/12/24*
1	Receive STRA and SSP from CONTRACTOR	
2	Complete draft SSI	
3	Receive approval from Rogun JSC for the SSI	
4	Produce audit timetable	
5	Assign roles and responsibilities to named individuals and record their acceptance of this	
6	SCR staffed and procedures practiced	
7	Training and Awareness of staff completed	
8	All Security Staff briefed on the Code of Conduct	

APPENDIX F -SECURITY INCIDENT REPORT

(To be Filled by the Contractor and Reviewed by the Consultant)

Contractor:	
Rogun JSC:	
City/Site/Location:	
Security Incident Report No: (Unique Site Code/Incident Number)	

Site Identifier:		**Category: (Highlight) >**	**Minor**	**Major**	**Critical**
Date of Incident:			Name of Reporting Officer:		
Time of Incident:			Name of Site Personnel Notified:		
Time Rogun JSC advised of Incident:			Name of Rogun JSC Officer Notified:		

Location: (Please Highlight/ Circle. If Other, please write in below.)	Internal to Construction Site		External to the Construction Site		N/A		
Google Maps Pin Drop Link (for all locations):							
Stakeholders Involved: (Highlight) – more than one can apply.	Local Police	Coast Guard	Border Guard	SFSP	Contractor	Rogun JSC person	Supplier
Other Stakeholder:							
Type of Incident:							
Description: Ensure Report includes **Who:** Who was involved **What:** What happened **Why:** Why did it happen **When**: When did it happen **How**: How did it happen **Actions:** Actions you undertook **Resolutions**: What did you do to resolve the incident **Notifications:** Who did you notify about the incident							

Summary Description Sequence of Events						
Follow Up Action Undertaken Following Incident (if none, N/A):						
Persons / Staff / Residents Involved:						
Name:		Department:			Involvement: (POI, Victim, Witness)	
Report Author:	Name:		Sign:		Time:	Date:

APPENDIX G - SITE SECURITY REVIEW

(To be Filled by the Contractor and Reviewed by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	
Monthly Site Security Review No: (Unique Site Code/Incident Number)	

Major Security Incidents Recorded		
Incident Type	**Date:**	**Resolved:**
Site Vulnerabilities Identified		
Site Location	**Vulnerability Description:**	**Remedial Security Action:**
Site Security Manager Comments:		
Rogun JSC Comments:		
Follow Up Action Undertaken (if none, N/A):		

Report Author:	**Name:**		**Sign:**		**Time:**	**Date:**

APPENDIX H - MONTHLY SECURITY INCIDENT REPORT

(To be Filled by the Contractor and Reviewed by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	
Monthly Incident Review Report No: (Unique Site Code/Incident Number)	

Contractor:		**Name of Reporting Officer:**	

Record of Incidents		
Incident Type	**Incident Quantities**	**% Increase / Decrease from Previous Month)**
Near-Miss		
Suspicious Activity		
Security Incident		
Response Report		
Response Type	**Response Quantities**	**% Increase / Decrease from Previous Month)**
No Response		
Report Filed		
Investigation		
On-site Security Response		
Escalation: External Agency		
Open / Closed Incident Report		
No. of Open Incidents		
No. of Closed Incidents		
Follow Up Action Undertaken (if none, N/A)		

Report Author	**Name:**		**Sign:**		**Time:**	**Date:**

APPENDIX I - SECURITY ROLE REQUIREMENTS

(To be Filled by the Contractor and Approved by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	
Monthly Incident Review Report No: (Unique Site Code/Incident Number)	

All personnel assigned to security duties should pass a criminal background record check.

Site Security Manager	
Minimum education requirement:	*Diploma or high school*
Minimum experience:	
• *10 (ten) years of police, security or military service.* • *Excellent oral and written communications skills and proficient in word processing, PowerPoint and spread sheets.* • *Minimum of 3 (three) years of experience in supervisory/managerial positions in a commercial customer facing role.* • *Minimum of 5 (five) years of experience in dealing/liaising with government organizations and international communities.* • *Preferred certification in an internationally recognized security qualification or accreditation, such as ASIS CPP.*	
Role	
This role involved establishing and managing the Security Management Plan on behalf of the site Contractors and providing senior management guidance to the Security Supplier, whilst managing the performance aspects of the contract for security services at the site. *This involves:* • *Day to day leadership of on-site security and incident management.* • *Advising the Contractors as appropriate on security for the site and its users.* • *Coordinate site security operations.* • *Liaise with external security and related stakeholders.* • *Maintain the site risk assessment and take relevant actions upon a change to the grading of a threat.* • *Leading investigation activity at the site.* • *Leading disciplinary activity for security staff, in conjunction with the Security Supplier.* • *Acting as the point of contact for security for Rogun JSC with regards to the site.* • *Reviewing and auditing security at the site.* • *Managing the training program for security staff and ensuring all training requirements are met.* • *Assisting security supervisors in the setting of weekly patrol patterns and routes.* • *Acting as the security lead for all VIP or other designated visits.* • *Managing the site user satisfaction program for security.* • *Be a member of the site emergency/crisis management team.*	

Security Supervisors

Minimum education requirement:	*Completion of secondary school*
Minimum experience:	
• *3 (three) years of progressive responsibility in managing a guard force.* • *5 (five) years of work experience as a security guard.* • *Good leadership skills and ability to exercise good judgment.* • *Trained at a minimum to have/show proficiency/knowledge in self-defense, report writing, occupational safety, threat evaluation, emergency and bomb threat response, protection of information, responding to emergencies, fire prevention and protection, legal aspects of providing security services, and radio/telephone communications.* • *Fluency in English (in case of expats facing role) (speaking/reading/writing).* • *Basic computer proficiency.*	
Role	
Security supervisors will: • *Manage security guards and their activities.* • *Assist in patrols, planning, reporting and gatehouse security duties as required.* • *Report to the Site Security Manager.* • *Assist security training activity.* • *Assist the Site Security Manager with customer satisfaction and complaints.* • *Collect and collate reporting information for daily, weekly and monthly reporting.* • *Assist in incident management including the coordination of the ICP and media holding areas.* *In addition, SCR supervisors will:* • *Manage SCR staff and their duties.* • *Assist with duties as required by the situation.* • *Be the primary point of contact for the SCR.* • *Prepare daily activity schedules, including access control enrolment sessions, virtual guard tours,* • *collation of guard tour system information.* • *Monitor reporting logs and the information included in them.* • *Act as the focal point for reporting damaged security infrastructure on the site.* • *Coordinate and communicate with external stakeholders as directed by the Site Security Manager.* • *Monitor real time events and escalate to the Site Security Manager as appropriate.* • *Control any information requests made to the SCR.* • *Ensure that shifts are properly manned with trained staff.* • *Ensure SCR information including mapping, overlays, policies and procedures are up to date and accessible to SCR staff.* • *Complete daily reporting duties ensuing that contractors inserts in the report logs are accurate and legible.*	

Security Guards	
Minimum education requirement:	*Completion of secondary school*
Minimum experience:	
• *2 (two) years of experience in security with a reputable organization.* • *Male or female candidates shall be accepted.* • *Minimum age of 21 years old.* • *Free from all communicable diseases and in good general health and physically and mentally capable of performing all the duties required of a security guard.* • *Drug dependency and medication: Shall not be dependent on alcohol or other drugs; if using prescribed medication, it shall not hinder the performance of assigned guard duties.* • *Elementary knowledge in English ability and fluency.*	
Role – Uniformed Site Duties	
The security guard will:	

- *Control site access and perform search and screening duties as required.*
- *Conduct site patrols as directed.*
- *Respond to alarms, alerts and taskings from either the security supervisors or Site Security Manager.*
- *Assist incident response.*
- *Maintain the required security logs and reports.*

Role – SCR Operator

In addition, the SCR Operator will:

- *Act as a communication link for security related matters.*
- *Operates SCR security systems.*
- *Conducts virtual site patrols via the camera system.*
- *Enrolls and maintains access control permissions as directed.*
- *Operates the site radio system base station, and ensures enough radios are charged and operable for each shift.*
- *Communicates with emergency responders.*

APPENDIX J - ACCOMMODATION CAMP ACCEPTABLE BEHAVIOUR

(To be Filled by the Contractor)

Contractor:	
Rogun JSC:	
City/Site/Location:	
Monthly Incident Review Report No: (Unique Site Code/Incident Number)	

The Contractor shall develop the Camp Code of Conduct & Rules, including relevant disciplinary actions, to be applied uniformly in all accommodations as applicable. The document will be translated into different languages to reflect the demographics of the Camp residents.

Residents will read and sign as having understood and agreeing to abide with the instruction provided.

The document will also be prominently displayed on the Camp notice boards, in different languages as applicable.

The section below highlights the minimum aspects that constitute Camp rules. The CONTRACTOR shall be responsible to develop and apply such requirements, expanding as applicable to all their Accommodation facilities for the entire duration of the project up to final demobilization.

The CONTRACTOR shall examine the rules included in the section below and integrate all relevant HR considerations required for disciplinary actions, in line with applicable company policies, labour laws and similar statutory regulations.

Rogun JSC reserves the right to inspect the CONTRACTOR'S camp facilities to verify compliance and adequacy with requirements.

Camp Acceptable Behaviour General Camp Rules

1. All Camp premises should be kept clean and tidy. The corridors and common areas are to be free from all personal items which may pose as an obstacle to cleaning work or be a fire safety hazard.
2. Residents should not throw rubbish, refuse or any other objects through windows or any part of the premises and should place such things into proper bins or containers or into the refuse skips provided within the Camp.
3. Residents are prohibited from installing any antenna on any part of the Camp accommodation or surrounds.
4. Residents should be properly dressed in public areas and common rooms of the accommodation and surrounds.
5. Residents are prohibited from keeping animals / pets in any part of the Camp accommodation or surrounds.

6. To prevent mosquitoes breeding, residents are prohibited from keeping plants in any part of the Camp accommodation or surrounds.

Inspections

Camp Management shall issue a “prohibited items list” and reserves the right for its designees to enter and inspect a room in the interest of health, safety and proper conduct of the occupant(s).

Entry will be made at any time, whether the occupant(s) are present or not, and without prior notice to the occupant(s). Any prohibited items or substances will be removed, and the cost of such items shall be the responsibility of the resident(s) who introduced the prohibited substance or item.

Entry during normal hours may also be made without prior notice, for the purpose of conducting non-emergency inspections, repairs and/or for the purpose of showing the premises.

Room Furniture

Each resident should check and report any missing or damaged furniture item(s) to the Camp Office not later than the following working day.

In the absence of this notification, it will be assumed that all furniture in the room is in good order, after which the resident(s) will be responsible for any subsequent loss or damage.

Accommodation Keys

Other than keys issued by the Camp Management to resident(s), duplication of keys is prohibited.

Any additional keys signed out from the Camp Office, should be returned to the Office on the same day.

Residents’ Belongings

Residents are advised not to keep large amounts of money and / or valuables in their rooms. Residents are reminded to lock their cupboard when they leave their room.

Camp Management will not accept any responsibility for the loss or damage of personal belongings.

Residents Code of Conduct

Each Camp Resident should conduct themselves in a polite manner and treat others as you would wish to be treated, which includes, but is not limited to, the following:

1. Respect other residents' personal, cultural and religious diversity.
2. Respect other residents' personal property. Each resident is responsible for the safekeeping of their personal valuables.
3. Residents should report any illness or accidents to the Camp Office immediately.
4. Residents should ensure that all garbage and waste materials are placed in the proper containers.
5. Residents should know the Camp Emergency Procedures to assist with any Emergency including Fire.
6. Any requests or complaints should be addressed to Camp Management.

Camp Rules

1. The Laws of the Republic of Tajikistan

The laws of Republic of Tajikistan are just as enforceable within the Camps as they are in the rest of the country. Accordingly, if a Camp resident breaks a Republic of Tajikistan law within the camp, the Authorities will be notified, and the resident will be subject to their disciplinary action.

As guidance, the following list includes, but is not limited to the kinds of actions that are contrary to Republic of Tajikistan law:

a. The possession, manufacture and / or consumption of alcohol.
b. The possession, manufacture and / or consumption/use of recreational drugs.
c. Organization of or participation in demonstrations and dissident actions.

Residents found breaking Republic of Tajikistan laws will be referred to the Civil Police.

2. Rooms and Surroundings.

a. Residents are prohibited from making any alternation to the premises or remove any fittings.
b. Residents are prohibited from installing main door locks of their own.
c. Residents are prohibited from displaying signs, posters or other objects on their accommodation doors. Residents will be liable for the cost incurred by the Camp Management for the removal of the objects or replacement of the doors.

d. Residents are prohibited from using double-sided tape, blue tack, concrete nails or other means for fixing objects to the furniture, windows, walls and doors of the room and surroundings. Residents will be liable for the cost in making good any damage done in the process of removing the displayed objects.

e. Residents will be liable for the cost in making good any damage to the building, property or fixtures and fittings in their accommodation deemed in excess of reasonable wear and tear and which in the opinion of the Management, falls into forgoing categories.

f. Residents are prohibited from dismantling any furniture provided and will be liable for the cost of assembling and restoring these items to their original condition.

3. Fire Fighting and Detection Equipment

a. Residents are prohibited from tampering with the Fire / Smoke detection sensors and equipment, including covering detectors.

b. Residents are prohibited from tampering with the firefighting equipment, including moving the equipment from its location or misuse such as use as a door stop.

4. Smoking

a. Smoking is not permitted in any part of the accommodation or other Camp premises.

b. Smoking is permitted only in designated areas.

5. Flammable Materials

Flammable liquids, explosive materials or combustible substances are not permitted in any part of the accommodation or other Camp premises or areas.

6. Naked Flames

a. Residents are prohibited from the use of flame cooking equipment including, but not limited to, gas cooking rings or camping gas stoves.

b. Residents are prohibited from any form of cooking in any part of the accommodation or other Camp premises or areas.

c. Naked flames, smoldering matter or smoking substance of any type are not permitted in any part of the accommodation or other Camp premises, including but not limited to candles and incense.

7. Use of Electrical Appliances / Energy Conservation

a. Residents are prohibited from the use of electrical cooking equipment including (but not limited to) electric cooking rings and kettles.

b. Residents are prohibited from any form of cooking in any part of the accommodation or other Camp premises.

c. Residents are to use only electrical accessories with correctly fitted plugs, such as 3 pin-plugs.

d. To ensure the safety of all users and to minimize nuisance electrical or power tripping, residents are prohibited from using multi-plug and extensions.

e. Residents are prohibited from using the power socket located outside their accommodation unit. These power sockets are used by the Camp staff for cleaning of common areas. The Camp Management will disconnect any plus contravening this requirement without any liability.

f. Residents should switch off all air-conditioning equipment, lights and electrical appliances when leaving their leaving room or when not in use.

Camp Residents should help conserve valuable energy and minimize energy wastage.

8. Residents Visitors

a. Residents shall comply with all visitor procedures implemented by Camp management.

b. Residents are strictly prohibited from hosting visitors of the opposite sex.

c. Any person caught residing overnight in the accommodation will be treated as trespasser and will be immediately removed from the Camp.

9. Occupancy / Exchange or Transfer Rooms

a. Residents are prohibited from exchanging or transferring their rooms without the prior approval of the Camp Management.

b. Residents are prohibited from allowing another person to take-over his room by residing under his name.

10. Noise Pollution

a. Residents are prohibited from excessive noise production, be it from music, TV, social gathering or other.

b. Residents are to keep all noise to a minimum between the quiet hours as communicated by Camp Management.

11. Security Staff

a. Residents are to adhere to any direction and / or instructions given to them by the Security Staff.

b. Residents should report any suspicious persons or objects found around the Camp immediately to the Security staff or directly to the Camp Security Operations room.

12. Vehicles, Driving and Passengers

a. Residents should adhere to any vehicle controls within the Camp, including travel direction, speed limits, parking restrictions and vehicle pass requirements.

b. Resident assigned as passengers to bus transport should adhere to any restrictions including, road crossing points, waiting line controls and pick-up / drop-off points.

13. Residents Criminality and Conflict

a. Residents caught committing a crime or theft of any nature will be referred to the Law Enforcement Authorities for their action.

b. Residents are prohibited from the harassment of any other resident or member of Camp Staff or visitors, including, but is not limited to, verbal or physical abuse.

c. Residents are prohibited from acting in a manner which may result in injury to another Camp resident or visitor or failing to reasonably protect another resident from being harmed.

14. Accountability, Identification card procedures

a. ID badges should be worn at all times while in the Camp, allowing Security Staff to identify authorized Camp residents.

b. Residents are prohibited to loan their ID card to anyone.

c. Residents are prohibited to photograph and / or reproduce their ID cards.

d. As per procedures, all Residents should scan their ID card whenever they are entering or leaving the Camp.

e. As per procedures, any loss or damage to the ID card will incur a charge for replacement. (deducted from salary)

f. In case of losing the ID card it should be immediately reported to the Camp Management.

g. Upon leaving the employment, ID card should be returned during clearance. (non-return deduction from salary will be applied)

15. Camp Rule Variations

If a resident is transferred to or has reason to visit another Camp to that originally assigned, and they should make themselves aware of any separate rules enforced within that Camp. Any Camp rule variations will be clearly displayed, along with the full rules, on notice boards throughout the Camp.

Disciplinary Actions

In the event of a resident's infringement of the Camp Rules, they will be liable for disciplinary action as detailed in the following table.

Rule Infringements	Action	Documented
First Offence	Reported to parent Company HR and responsible management	First Warning Letter from HR issued to offender, recorded in Camp offenders' records
Second Offence	Reported to parent Company HR and responsible management	Second Warning Letter from HR and deduction of pay. Recorded in Camp offender's records
Third Offence	Reported to parent Company HR and responsible management	Final Warning Letter from HR, increased deduction of pay issued to offender recorded in Camp offender's records

Fourth Offence	Reported to parent Company HR and responsible management	Removal from the project

Serious Misconduct and significant infringements of the Camp Rules, including fighting, may result in summary dismissal and immediate release from the Project.

Declaration:

I have read, understood and will adhere to the Accommodation Camps Code of Conduct, Rules and Disciplinary Actions:

Name:			
Badge No:			
Company:		ID No:	
Date:		Signature:	

APPENDIX K - SITE SUITABILITY ASSESSMENT REPORT TEMPLATE

(To be filled by Contractors and approved by the Rogun JSC)

Site Suitability Assessment Report					
Contractor		**Site Name**		**Date**	
Location		**Rogun JSC**			

PURPOSE & OBJECTIVE

The purpose of a site suitability assessment is to ensure the safety, protection, and resilience of a project. This assessment serves as a meticulous examination aimed at evaluating the compatibility of the site with security requirements. Its primary purpose lies in identifying potential security risks, vulnerabilities, and threats that may compromise the integrity of the site, its occupants, and assets.

SITE OVERVIEW

Details about the site include but are not limited:

- *Location details*
- *Size and layout of the site*
- *Surrounding environment (urban, suburban, rural)*
- *Overview of existing structures or infrastructure*

ACCESS CONTROL

Assess access control of the site. A few examples are mentioned below:

- *Assessment of current access points to the site*
- *Evaluation of access control measures (e.g., gates, locks, security personnel)*
- *Recommendations for improving access control before work*
- *Details Strengths and weaknesses of the site from a security perspective.*

PERIMETER SECURITY

Assess the perimeter security of the site. A few examples are mentioned below:

- *Inspection of perimeter fencing or barriers*
- *Analysis of potential breaches in perimeter security*
- *Suggestions for enhancing perimeter security measures*

SURVEILLANCE SYSTEM

Assess the surveillance system of the site. A few examples are mentioned below:

- *Review of existing surveillance systems (e.g., CCTV cameras)*
- *Assessment of monitoring capabilities (e.g., security personnel, remote monitoring)*
- *Recommendations for improving surveillance and monitoring coverage*

SECURITY LIGHTING

Assess the security lighting of the site. A few examples are mentioned below:

- *Examination of lighting conditions at the site*
- *Identification of poorly lit areas that may pose security risks*
- *Suggestions for installing or upgrading security lighting*

EMERGENCY PREPAREDNESS

- *Evaluation of emergency response procedures*
- *Assessment of emergency communication systems*

RISK ASSESSMENT

Conduct a risk assessment of the site. Refer to ISO 31000- Risk Management

- *Identification of potential security risks associated with the planned work*
- *Analysis of the likelihood and impact of each risk*
- *Recommendations for mitigating identified risks*

COMPLIANCE WITH SECURITY MANAGEMENT PLAN

Assessment of the site's compliance with *Security Management Plan*

FINDINGS AND RECOMMENDATIONS

Summary of key findings from the assessment

APPENDICES

List additional supporting documentation (e.g., maps, diagrams, photos)

REFERENCES

Citations for any sources or references used in the report such as ISO 31000-Risk Management

DOCUMENT RECORD

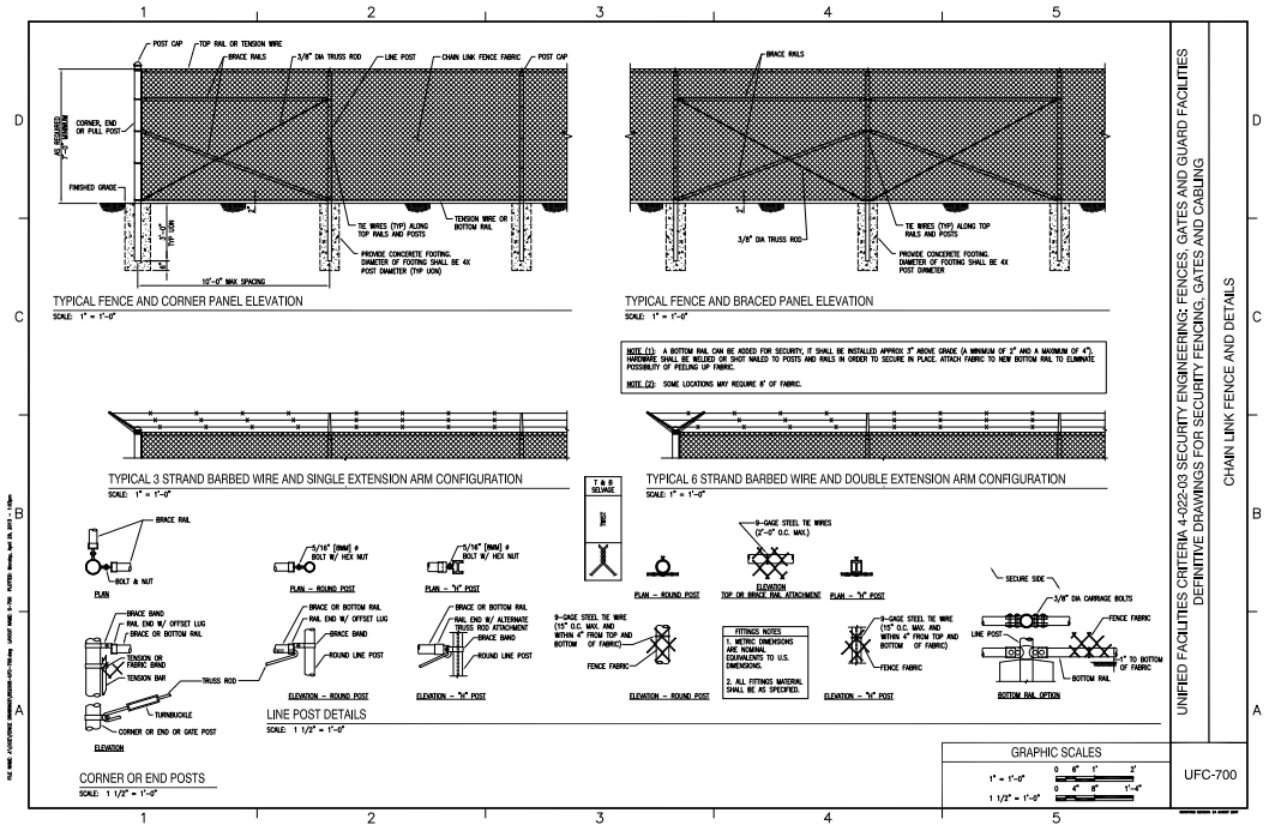
REVISION	DRAFTED BY	INTIAL DRAFT OR LIST AMENDMENTS	APPROVED BY	DATE

APPENDIX L - CHAIN LINK FENCING AND DETAIL

(US DEPARTMENT OF DEFENSE UFC 4-022-03 1 OCTOBER 2013 UNIFIED FACILITIES CRITERIA SECURITY FENCES & GATES)

(To be Filled by the Contractor and Reviewed by the Rogun JSC)

Contractor:	
Rogun JSC:	
City/Site/Location:	

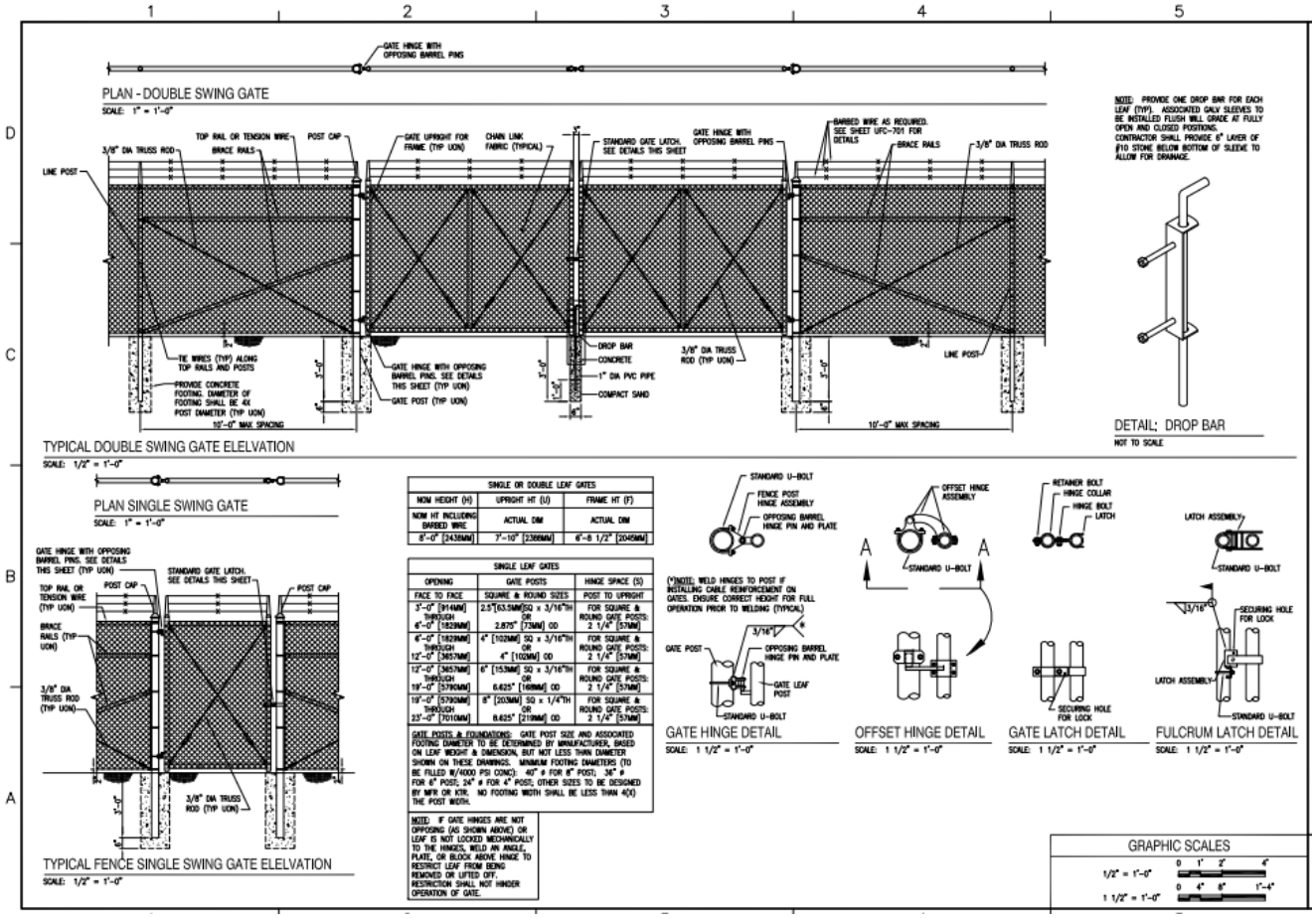


APPENDIX M - CHAIN LINK SWING GATE AND DETAILS

(US DEPARTMENT OF DEFENSE UFC 4-022-03 1 OCTOBER 2013 UNIFIED FACILITIES CRITERIA SECURITY FENCES & GATES)

(To be Filled by the Contractor)

Contractor:	
Rogun JSC:	
City/Site/Location:	



APPENDIX N - GBV-SENSITIVE CODE OF CONDUCT FOR SECURITY PERSONNEL

Purpose

This Code of Conduct outlines the expected behavior of all security personnel assigned to the project. It aims to ensure the safety, dignity, and rights of all individuals—particularly women, children, and vulnerable groups—through a zero-tolerance approach to Sexual Exploitation, Abuse, and Harassment (SEAH/GBV).

1. General Conduct

Security personnel shall:

- Conduct themselves with the highest level of integrity and professionalism at all times.
- Treat all individuals with respect, dignity, and fairness, regardless of gender, age, nationality, religion, ethnicity, or background.
- Comply with applicable laws, the Security Management Plan (SMP), international standards, and this Code of Conduct.

2. Prohibited Behaviors

- Security personnel shall not:
- Engage in any form of sexual harassment, exploitation, or abuse.
- Engage in transactional sex, including the exchange of money, employment, goods, or services for sex or sexual favors.
- Touch, search, or speak to individuals in a sexually suggestive or disrespectful manner.
- Engage in relationships with community members that may be perceived as exploitative or coercive, especially with minors or individuals under their authority.
- Use threats, intimidation, or coercion, particularly toward women and children.
- Use language or gestures that are abusive, discriminatory, or sexually inappropriate.

3. Responsibilities

Security personnel shall:

- Report any observed or suspected incidents of SEA/GBV or misconduct immediately, using the established reporting channels.
- Support victims by directing them to appropriate grievance mechanisms or support services without discrimination or delay.
- Cooperate fully with investigations and any corrective or disciplinary measures taken.
- Protect the confidentiality of survivors and individuals involved in reporting or investigation.
- Participate in mandatory GBV training, including refresher sessions.

4. Whistleblower Protection

All personnel are protected from retaliation for reporting SEA/GBV in good faith. The project guarantees confidentiality and support for whistleblowers in line with the project's grievance and whistleblower policy.

5. Disciplinary Measures

- Violations of this Code may result in:
- Immediate removal from duty or site.
- Termination of employment or contract.
- Legal action in accordance with applicable laws.
- Reporting to relevant authorities, including the police, where criminal behavior is involved.

6. Acknowledgment

I, the undersigned, acknowledge that I have read, understood, and agree to adhere to this GBV-Sensitive Code of Conduct. I understand the consequences of non-compliance and my responsibility to uphold the safety and dignity of all individuals at all times.

Name: _____

Position: _____

Signature: _____

Date: _____