



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

Alfa Security Terms and Conditions for Third Party



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

TABLE OF CONTENTS:

1. Guide and Scope	3
2. Abbreviations and Definitions	3
2.1 Abbreviations	3
2.2 Definitions	4
3. General Terms	4
4. Physical Access	6
4.1 Switches	6
4.2 External Sites of MIC1 Network	7
5. Logical Access	7
6. Local Access	9
7. Remote Access: Networks Interconnection	10
8. Network, Systems and Solutions	10
9. Remote Networks Connectivity	12
10. Additional Security and Compliance Clauses	13



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

1. Guide and Scope

This document is addressed to all MIC1's suppliers and contractors. It should be attached to any NDA (non-disclosure agreement) or contract that will be signed between MIC1 and any contractor or supplier. It should be also signed by any supplier wishing to participate in a bid.

The document defines the security requirements that MIC1's contractors, sub-contractors and partners should comply with when dealing with any part of MIC1's IT/Technology equipment, applications, or data.

Furthermore, the document includes a list of security requirements that should be included in every project requiring a physical or logical access to MIC1 infrastructure. These requirements aim to ensure secure access and protect MIC1's assets.

2. Abbreviations and Definitions

2.1 Abbreviations

ASAP	As Soon As Possible
CIO	Chief Information Officer
CTO	Chief Technology Officer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GDPR	General Data Protection Regulation
ID	Identity
IIO	IT Infrastructure Operations Entity
IT	Information Technology
ITI	IT Infrastructure Department
LAN	Local Area Network
MIC1	Mobile Interim Company 1
NDA	Non-Disclosure Agreement
NOC	Network Operations Center Entity
OS	Operating System
PC	Personal Computer
PoP	Point of Purchase
PoS	Point of Sale
SIM	Subscriber Identity Module
Sr.	Senior
SSLM	Supervision and Service Level Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

WINS	Windows Internet Name Service
WLAN	Wide Local Area Network

2.2 Definitions

Alfa: It is the brand name owned by Mobile Interim Company 1 SAL (MIC1) which is managing a Lebanese mobile network for the benefit of the Republic of Lebanon / Ministry of Telecommunications.

Contractor: Generic term defining the party (customer, connectivity provider, partner, supplier, or contractor) contracting with MIC1 under the term of this agreement.

Contractor's collaborators: Every person working for the contractor, whatever directly or indirectly. This includes individuals under direct contact with the contractor (such as employees, interims, students, consultants) as well as any person employed directly or indirectly by the contractor's sub-contractors.

Interactive accesses: Accesses to human-to-machine interfaces, executed by a physical person via a workstation (PC or system terminal). Contrary of machine-to-machine communications, running in automatic mode without needing any human activity.

Strong password: A password compliant with following rules:

- At least eight characters consisting of three from the following combination:
 - At least one capital letter: [A-Z]
 - At least one small letter: [a-z]
 - At least one number: [0-9]
 - At least one special character: @, \$, *, ?, ...etc.

3. General Terms

This section provides details on the security requirements and associated liabilities related to the contractor's access, whether physical or logical, to MIC1's information, applications, and systems. It also pertains to the delivery of IT/Technology solutions and services by the contractor to MIC1.

The following points outline the expectations and procedures:

1. The contractor should ensure strict compliance with all the requirements described here at all times.
2. Failure to comply with the requirements outlined below holds the contractor responsible for any resulting loss or damage.
3. It is the contractor's responsibility to inform all of its collaborators about the terms and requirements of this contract schedule and ensure their full compliance as well.
4. MIC1 reserves the right to verify the contractor's compliance with the security requirements stated in this document, a maximum of twice a year, using the following method:
 - a. If available, the contractor can provide MIC1 with the report from its most recent security audit conducted by an external, independent auditing company.
 - b. If such a report is not available, cannot be disclosed, or is deemed unsatisfactory by MIC1, MIC1 may request a specific security audit of the contractor if necessary. This audit, conducted at MIC1's expense, should be carried out within ten (10) working days after the contractor receives MIC1's request. It will be performed by an independent security auditing



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

company, agreed upon by both parties, and should not be a direct competitor of the contractor. The contractor should provide the accredited auditor with access to any area, equipment, document, or information related to the contractor's mission for MIC1. The auditor should prepare an audit report and present it to both MIC1 and the contractor. The parties should then decide on a reasonable grace period during which the contractor can address any reported shortcomings. MIC1 has the right to request a follow-up audit after this grace period, which will not count towards the "twice a year" limit for audits.

- c. In the case of onsite presence, the contractor's PCs may be subject to inspection.
5. If, at any time and for any reason, the security requirements are not met, MIC1 will notify the contractor, and the contractor will be granted a grace period, which will be mutually agreed upon and approximately in the range 6 months, to rectify the situation. If the identified shortcomings are not addressed within this period, MIC1 reserves the right to revoke the Contractor's physical and logical access to its systems and premises.
6. MIC1 reserves the right to temporarily suspend the contractor's logical accesses, after notifying the contractor, if the contractor's equipment is compromised and poses a significant direct security risk to MIC1. Examples of such risks include viral infection, data theft, data loss, data corruption, or external intrusion on the contractor's equipment.
7. All equipment provided by MIC1 to the contractor and its collaborators (e.g., Security ID cards, SIM Cards, tokens, networking equipment, and workstations) remain the property of MIC1 and should be returned upon the completion or termination of this contractual relationship.
8. The contractor should take appropriate the measures to protect the MIC1 equipment provided to them and their collaborators against theft, loss, and damage.
9. The contractor should take all necessary actions to prevent damage, whether physical or logical, to MIC1 assets (including network, hardware, software, data, and brand image) caused by the contractor's equipment and solutions, sub-contractors' equipment, and contractor's collaborators. This includes preventing data losses, data corruptions, and service interruptions resulting from the following:
- Misconfigurations, errors, misconduct, false-operations, and voluntary data alterations.
 - Spreading of viruses, Trojans, backdoors, or any other form of malicious code that may occur through the contractor's collaborators, contractor's equipment and solutions or contractor's sub-contractors' equipment (such as workstations, servers and networking equipment).
 - Software running on contractor's or contractor's sub-contractors' equipment (such as workstations, servers, and networking equipment) that disrupts the normal operations of MIC1's infrastructure.
 - Usage of insecure communication links or protocols between their equipment/solutions.
 - Non-compliance with MIC1 password policy, specifically regarding:
 - The use of strong passwords.
 - Prohibition of hardcoded passwords, enabling default username/password, sharing passwords with unrelated individuals, or setting passwords to "Never Expire."
 - Changing all system-level passwords (such as root, Windows, and application administrators) at least quarterly, and all other accounts on a monthly basis.
 - Ensuring that passwords are always communicated securely.
10. The Contractor should take all reasonable measures to prevent misuse of tools, including Internet tools like e-mail address and web surfing access that may be provided by MIC1 to the contractor's collaborators. MIC1 reserves the right to suspend access if any misuse is detected.



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

4. Physical Access

The guidelines below apply only when all or parts of contract's mission require contractor's collaborators to work inside MIC1 premises or switches.

All Contractors' collaborators who need to work inside MIC1 premises should be individually and formally registered through the following procedure:

1. Contractor should send to MIC1 a list of all collaborators who will need access to MIC1 premises. For each collaborator, the following information is required: Surname, first name, and degree of access frequency (e.g., every day, once per week, backup of somebody).
 - a. Case 1 – For individuals who require regular access to MIC1 premises for a duration exceeding 3 months, a pre-identified person (as described above) should be granted temporary access to specified areas based on their job requirements.
 - b. Case 2 – For individuals who visit MIC1 premises occasionally, each pre-identified person (as described above) should be required to present their national identity card or passport to the MIC1 reception agent during each visit. Upon verification, the person will be issued a visitor badge. When the person departs from the MIC1 building, the visitor badge should be returned. The contractor's collaborator should be escorted in MIC1 premises by a MIC1 team member from the reception to their office or meeting room, and then back to the reception after the visit is finished.
2. Any person who has been issued a badge should wear it in any plain view at any time. The badge should be worn for identification in all areas. A badge is individual and cannot be lent; it can only be worn by its owner. The owner is responsible for any misuse of his badge and should report a lost badge immediately.
3. At the end of the contract or when a person's presence is no longer required at MIC1 premises, all security access badges should be returned at MIC1 reception.
4. For business visits after regular working hours, a permission from the manager of the MIC1 Contact person is mandatory. This permission should be issued by the designated MIC1 contact person and made available to the Safety Compliance department for record-keeping and verification purposes.
5. All the pre-mentioned regulations are applied in all MIC1 locations (Parallel Tower, Libatel, Pine, and Justice, as well as all PoS and PoP) in addition to extra measures depending on the nature of each location which are clarified hereafter.

4.1 Switches

This section is addressed to contractors who need to access MIC1 switches and datacentres:

1. A comprehensive list containing the names of all collaborators who require access to the switch should be provided by the contractors. This list should be granted access as per the internal policies and procedures.

The provided list should specify the time and duration of the non-MIC1 employees' missions, and it should be updated every 3 months. In the event of any modification to the list, MIC1 contact person should be notified immediately to proceed with necessary approvals as per the internal policies and procedures.

Furthermore, the contractors' interventions on site, whether during the day or at night, should always be performed in the presence and supervision of MIC1 personnel.



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

2. In case there is a need for someone outside the approved access list to gain access to the switch, MIC1 contact person should be notified to get appropriate approvals.
3. In the event that the access request is made during non-working hours, the requestor from MIC1 side should contact the Safety Compliance department team directly to grant access.
4. Inflammable materials should not be kept inside the switches.
5. Contractor's collaborators should only utilize the main entrance doors when accessing the switches. The use of any other doors is prohibited.
6. Smoking is prohibited inside the switches.
7. Food and drinks are prohibited inside the switches.
8. The use of machines producing sparks or heat inside the switches should be reported in advance to MIC1 representative or contact person to take the necessary precautions and report the case to concerned entities within MIC1.

4.2 External Sites of MIC1 Network

This section is addressed to contractors who requires access to MIC1 network external sites:

1. Contractors' employees should present their company IDs and National IDs to the local guard and record their information and task in the logbook as well as the guard book (Where applicable).
2. The contractors' employees should ensure that the shelter and the fence doors are securely closed before leaving the site. They should also maintain site cleanliness by removing any flammable materials or unused items. Prior to entering and leaving the site, every intervener should contact the NOC team on 03391313 to update the site access database.
3. No individual should take any item out of the site without obtaining prior approval of MIC1. Such an approval should be obtained through an e-mail received from the designated MIC1 contact person.
4. Site should be opened with its key. Any attempt to break the lock or climb the fence is strictly prohibited, regardless of the reason.
5. The Contractor should provide the MIC1 project manager or contact person with a comprehensive list containing the names of all the contractor's employees who require access to the sites, along with their respective phone numbers.
6. Contractors should exercise caution when refilling diesel tanks, and any leaks should be promptly addressed, and the spot cleared.

5. Logical Access

The clauses in this section should apply specifically when the contractor needs to access MIC1 systems, applications or data, whether it is done locally within MIC1 premises, or remotely from any non-MIC1 location.

1. Any information hosted on MIC1 systems, should be considered as confidential, and as such covered by the terms of this document confidentiality clauses. In all cases, this information remains MIC1 property.



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

2. The Contractor's collaborators should receive a temporary password which will be valid for one time access only, and it should be changed after intervention completion.
3. All forms of logical access identification media provided to the contractor, including logins, Secure ID cards, soft tokens, and authentication keys, should be used at least once every 3 months. Failure to use any of these media within this timeframe may result in automatic disabling without prior notification to the contractor. Such action does not prejudice the rights or liabilities of MIC1.
4. The Contractors' collaborators should use the devices, software and access rights provided to them by MIC1 only for the purpose of fulfilling their mission. Typically:
 - a. They should not use the provided Internet access tools (e-mails and web surfing accesses) for any other purpose than the ones related to this mission.

Note: Inside MIC1, the internet access filtering is implemented to restrict access to non-ethical sites. The term "non-ethical site" encompasses various types of content that may pose a risk to MIC1 or involve a violation of laws, particularly those related to harassment and racism. This includes but is not limited to websites that distribute inappropriate or offensive content.
 - b. They should comply with the access rights provided to them by MIC1, and they should not try to execute actions which would bypass these provided access rights.
 - c. They should not execute actions (like install or use of software) that would infringe software licensing policies or violate digital property regulations.
5. Unless explicitly required for the execution of the mission described within the scope of this contract, contractors' collaborators should refrain from making any changes to access rights or creating user accounts on the accessed systems or applications without prior written permission from their MIC1 technical contact. Furthermore, contractors' collaborators should not take advantage of any granted privileges or proprietary data that may exist on MIC1 systems, unless explicitly permitted in writing by their MIC1 technical contact.
6. Any device used by the contractor and its collaborators to access the MIC1 private data network (including, but not limited to, users' workstations, servers, network equipment) should be:
 - a. Secured with strong passwords.
 - b. Locked to prevent any access when the work area is left unattended.
7. Any device owned by the contractor or its subcontractors that establishes direct or indirect connections to the MIC1 network, including users' workstations, servers, and routers) should adhere to the following requirements (if applicable):
 - a. It should have valid licenses for all software installed on it.
 - b. It should be physically and logically protected to prevent unauthorized use by individuals other than MIC1's or contractor's collaborators.
 - c. It should be properly configured and secured in accordance with the state-of-the-art IT security practices.
 - d. It should not run any software that could interfere with MIC1 infrastructure. For instance:



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

- I. Workstations should have up-to-date anti-virus and personal firewall or personal intrusion detection software.
 - II. Servers and workstations access should be protected using strong password.
 - III. Servers and workstations directly communicating with the MIC1 private network should not run any network information service or network dynamic configuration service that could interfere with similar services provided by MIC1 (such as DHCP, DNS, WINS or dynamic routing information services).
 - IV. Servers and workstations directly communicating with MIC1 private network should not run applications that put MIC1 equipment at risk (e.g., network scanners or vulnerability detection software).
- e. It should use secure connections when establishing connections to the MIC1 network.
8. If the contractor detects/identifies any security exposure, misuse, or non-compliance situation, they should promptly contact the designated MIC1 contact person. The MIC1 contact person will then be responsible for notifying the concerned entities regarding the issue.
 9. If the contractor becomes aware of the loss or theft of any provided MIC1 asset that has been provided to them, they should immediately contact the designated MIC1 contact person. The MIC1 contact person will then take appropriate action and follow the necessary protocols, which include contacting the security hotline for reporting the incident.
(MIC1 Security hotline number: +961 3 391112)
 10. The contractor agrees and commits not to misuse the provided accesses for obtaining information about MIC1's business, customers, or partners that falls outside the scope of the mission described in this contract. This includes refraining from intercepting or monitoring communications conducted internally within MIC1 or with other contractors, partners or customers of MIC1.
 11. All connection sessions to MIC1 network, equipment and applications are subject to monitoring and logging by MIC1. The contractor is hereby informed that these log records may be utilized as evidence in the event that MIC1 needs to enforce a claim brought against the contractor for failure to comply with its obligations. If such log records are to be used as evidence, the contractor should be granted access to them to assess the case.
 12. Upon termination of the contractual relationship termination, the contractor should return to MIC1 any data that were provided to them that are considered MIC1 property. This includes copies of databases, project information files, and any other data that were entrusted to the Contractor during the course of the contract. Additionally, the contractor should permanently erase any copies of these data that may have been stored on their equipment such as workstations, servers and backup devices.

6. Local Access

The Clauses in this section are only applicable when the contractors' collaborators are operating within MIC1 premises including office spaces or technical sites.

1. The Contractor's collaborators should not connect any equipment that is not provided by MIC1 to the MIC1 private data network without a prior approval by email from their MIC1 technical contact person.
2. Access to MIC1 systems should be performed through a MIC1 owned workstation.



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

3. If non-MIC1 equipment is authorized to be connected to the MIC1 private data network, the following requirement should be met:
 - a. The equipment should be registered with the MIC1 Service Desk via a Request For Change
 - b. The equipment should be equipped with an up-to-date anti-virus software and operating system.
 - c. The equipment should be protected from theft by the contractor.
 - d. The equipment should undergo viruses and vulnerabilities scanning by the IIO entity for approval to be connected to the WLAN and LAN. It should have a certified up to date anti-virus installed on that laptop, the latest OS patches installed, and no vulnerabilities present.
4. The contractors' collaborators should comply with all MIC1 Information Security Policies published on MIC1 intranet web site and available upon request.
5. Visitors/consultants who only requires access to e-mail and internet should utilize the wired/wireless guest VLANs.
6. When connected to the MIC1 WLAN, bridging between wired and wireless access is not permitted. The contractor collaborators should not use any tunnelling software that provides access to any external network. The ITI department have the right to block any such connectivity when discovered.

7. Remote Access: Networks Interconnection

Clauses in this section are applicable only when there is a need to establish a network interconnection between MIC1 and the contractor's (or subcontractor's) networks. This interconnection may involve accessing MIC1 internal applications and systems from a remote location.

1. The contractor's network and devices, directly or indirectly connected to the MIC1 network, should not have any non-filtered network connections to third party networks or equipment (for instance the Internet or another private network). The term "Filtered" implies that the connections are controlled by at least properly managed firewall equipment.
2. The contractor should strictly limit access to its equipment directly or indirectly connected to MIC1 network. Only individuals required for fulfilling this contract's mission should be granted access to this contractor's equipment.
3. The contractor, including its collaborators, should memorize passwords allowing access to any contractor's equipment connected directly or indirectly to MIC1 systems. This includes the passwords of equipment used to setup the remote access connection such as VPN gateways, firewalls router, etc. Under no circumstances should these passwords be visibly written down on devices.
4. For interactive accesses, the contractor's collaborator should always disconnect from the MIC1 target systems upon completion of their tasks. Additionally, the system will disconnect after 10 minutes of inactivity.
5. MIC1 will implement all reasonable measures to prevent any unauthorized access to the contractor network through the interconnection. The contractor should also take all reasonable measures to protect its IT infrastructure from illegitimate accesses.
6. Under no circumstances are dial up connections permitted to internal MIC1 systems.

8. Network, Systems and Solutions

The following requirements apply for all contracts involving IT and Network solutions development, delivery, installation, support, and operation:



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

1. The contractor should comply with MIC1 Change Management Procedure. This procedure is available upon request. Practically, any intervention that involves changing an equipment hardware, software or configuration should be communicated in advance to the MIC1 technical contact. The MIC1 technical contact is responsible of issuing the request for change via MIC1 change management system. The intervention can only proceed after the validation of the request for change ticket by the impacted teams. Requests should be submitted 48hours prior to the scheduled change for proper assessment and approvals. Changes should be planned, tested, and implemented in a controlled manner to minimize disruptions and security risks.
2. The contractor should obtain explicit written authorization from their MIC1 correspondent before executing any change that may compromise the security level of the equipment and/or service related to this contract's scope, or of any other MIC1 equipment or service. It is the responsibility of the MIC1 correspondent to evaluate such changes in agreement with the MIC1 Information Security department.
3. Every intervention, whatever planned or executed in emergency, should be documented in an intervention report. This report should be sent via e-mail to the MIC1 technical contact person, who will follow the appropriate procedure. The intervention report should include:
 - a. Starting & ending time and date of the intervention
 - b. Purpose of the intervention
 - c. Linked trouble ticket, intervention or change request
 - d. Main actions executed
 - e. Problems encountered and solutions applied
 - f. Global result
4. Any information or data available or obtained by the Contractor during the execution of this contract such as dump files, database extracts, etc.:
 - a. Should only be used only in the scope of this contract's mission.
 - b. Should be retained only for the duration necessary to complete the required intervention and should be permanently destroyed by the contractor thereafter.
 - c. Should be treated as confidential and protected by the confidentiality clauses of this contract.

Moved systems:

In the event that the contractor is required to move MIC1 systems outside MIC1 premises to execute their mission, the contractor should ensure that all systems moved outside MIC1 premises are adequately covered by an insurance contract as long as they remain under the contractor's responsibility. This insurance contract should cover any losses, including theft, physical, or logical damage such as data loss or corruption.

The contractor is permitted to create backups of the data and software hosted on the moved systems for backup purposes during the intervention. These backups should be stored securely within MIC1 premises and protected against unauthorized access. All backup copies should be erased once the MIC1 technical contact confirms that the systems have been returned to MIC1 premises and the need for backups is no longer necessary. The provision of backups to the contractor should only with exceptional approval. Contractors should commit to not offer, instal, or utilize any equipment which may pose a security threat, or compromise MIC1 network security.

5. All vendors, contractors, sub-contractors are strictly prohibited from taking photographs inside MIC1 critical sites and premises unless approved by MIC1.
6. When applicable, to prevent any 3rd party laptops from being directly connected to the MIC1 network, administrator' rights should not be granted.



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

7. All Solutions offered by the supplier should comply with the following requirements to ensure security and non-jeopardization of the MIC1 environment:
- Application should run without the need for root (UNIX) or administration (Windows) privileges.
 - Applications should support the installation of an Antivirus and its updates.
 - Operating system, database and application administrator users should be separate.
 - Systems should support a patching mechanism that allows the deployment of the most recent security patches by the contractor (upon MIC1 request) or by MIC1, without interfering with the applications, within a timeframe set by MIC1.
 - Solutions should comply with MIC1's Password policy in particular:
 - The use of Strong password.
 - The prohibition of hardcoded password, enabling default username/password, sharing the password with business unrelated persons, and setting the password to "Never Expire."
 - All System-level passwords such as root, Windows, and applications administrators, should be changed at least quarterly, while other accounts passwords should be changed monthly.
 - Passwords should always be communicated in a secure manner.

Failure to comply with the above requirements holds the supplier/contractor fully responsible of any malware spread including viruses, worms, Trojans, or botnets resulting in damage, disruption, data theft, or any other unauthorized actions affecting MIC1 data, hosts, or networks.

If investigations determine that the network malware originated from any of the systems and solutions supplied by the contractor, the contractor should promptly cooperate with MIC1 team to remove the malware and provide indemnities for the assessed damages caused by the incident.

9. Remote Networks Connectivity

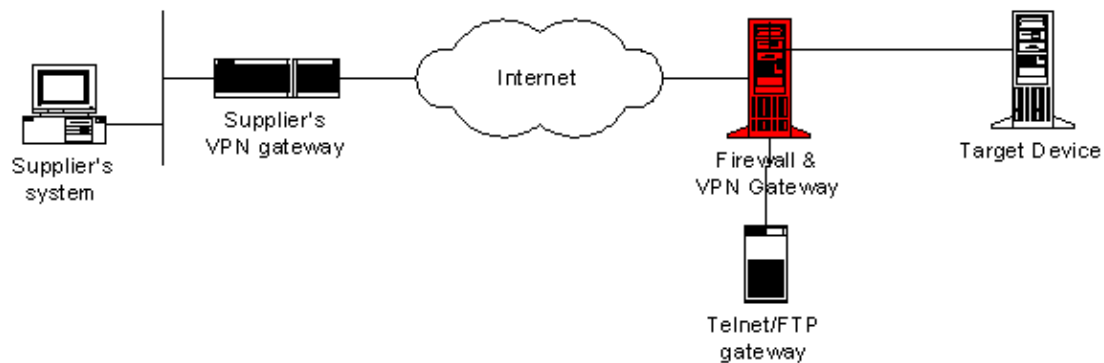
The networks connectivity refers to the technical setup established to facilitate the communication between the contractor's systems or collaborators located outside of MIC1 premises and MIC1 equipment. This connectivity is implemented on-demand and is only activated upon request. However, it is important to note that remote connectivity is not approved for suppliers that have a local presence in Lebanon as they should perform all activities on site. Initial installations should be conducted by suppliers on site even if they do not have a local presence. Remote connections may be permitted for support purposes after the issuance of acceptance.

The only approved method for remote connectivity is the "LAN-To-LAN IP VPN over Internet." This method utilizes the following architecture:



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023



The Contractor's VPN gateway can either be a firewall, or a dedicated VPN box.

Both parties, the contractor and MIC1, should complete the MIC1 Template for connection requirements before establishing any connection.

10. Additional Security and Compliance Clauses

This section presents additional security and compliance clauses that are essential for all MIC1 suppliers and contractors.

1. **Compliance with Applicable Laws and Regulations:** The contractor and its collaborators should comply with all relevant laws, regulations, and industry standards pertaining to information security, data protection, privacy, and intellectual property rights. This includes but is not limited to compliance with the General Data Protection Regulation (GDPR), applicable local data protection laws, and any other relevant international standards or regulations.
2. **Confidentiality and Non-Disclosure:** The contractor and its collaborators should maintain the confidentiality of all MIC1's proprietary information, trade secrets, customer data, and any other confidential or sensitive information obtained during the course of their engagement with MIC1. This obligation should extend beyond the termination of the contractual relationship.
3. **Security Incident Reporting:** The contractor should promptly report any security incidents, breaches, or suspected breaches to the designated MIC1 contact person. This includes unauthorized access, loss or theft of data or equipment, malware infections, and any other security-related incidents. The contractor should cooperate fully with MIC1 in investigating and mitigating such incidents.
4. **Security Awareness and Training:** The contractor should ensure that its employees and collaborators receive adequate security awareness and training on information security best practices, policies, and procedures. This should include regular training sessions and awareness campaigns to educate personnel about potential risks, social engineering attacks, phishing attempts, and the proper handling of sensitive data.
5. **Data Handling and Protection:** The contractor should implement appropriate technical and organizational measures to protect MIC1's data and ensure its integrity, confidentiality, and availability. This includes encryption of sensitive data in transit and at rest, secure storage and disposal of data, regular backups, access controls, and secure coding practices.
6. **Subcontractors and Third-Party Vendors:** If the contractor engages subcontractors or third-party vendors to perform any services related to MIC1's IT/technology equipment, applications, or data, the contractor should ensure that these entities comply with the same security requirements and obligations outlined in this document. The contractor should be held responsible for the actions or omissions of its subcontractors or third-party vendors.
7. **Business Continuity and Disaster Recovery:** The contractor should have appropriate business continuity and disaster recovery plans in place to ensure the continuity of services in the event



Alfa Security Terms and Conditions for Third Party

Reference Number	SF-CF-107
Owner	PRO
Revision Code	1.0
Implementation Date	October 2023

of unforeseen disruptions, disasters, or incidents. These plans should address data backup and recovery, system restoration, alternative site arrangements, and communication protocols.

8. Termination and Transition: In the event of contract termination, the contractor should cooperate with MIC1 to ensure a smooth transition of services and the secure handover of all MIC1's data, systems, and equipment. This includes returning all MIC1-owned assets, removing access privileges, and securely erasing any data or configurations associated with MIC1's systems.
9. Indemnification: The contractor should indemnify and hold MIC1 harmless from any claims, damages, losses, liabilities, and expenses arising from the contractor's failure to comply with the security requirements or any security incidents caused by the contractor's negligence, willful misconduct, or breach of obligations.
10. Amendments and Updates: MIC1 reserves the right to amend, update, or modify these security terms and conditions at any time. The contractor should be notified of any changes, and their continued engagement with MIC1 should be deemed acceptance of the revised terms and conditions.

Supplier/Contractor Name: _____

Authorized Representative Name: _____

Authorized Representative Signature: _____

Date: _____