

# MIC1 Security Terms & Conditions for Suppliers and Contractors

## **Table of contents**

<b>2.</b>	<b><i>Abbreviations and definitions</i></b>	<b>3</b>
<b>3.</b>	<b><i>Instructions</i></b>	<b><i>Error! Bookmark not defined.</i></b>
3.1	General Terms:	4
3.2	Physical Access:	5
3.3	Logical Access:	7
3.4	Local Access:	8
3.7	Networks Connectivity Requirements:	10

## 1. Guide and Scope

- This document is addressed to all MIC1's suppliers and Contractors; it will be attached to any NDA (non-disclosure agreement), contract that will be signed between MIC1 and any Contractor/ supplier. It will be also signed by any supplier wishing to participate in a bid.
  - It defines the Security Requirements that MIC1's contractors, sub-contractors and partners shall comply with, when dealing with any part of the MIC1 IT/Technology equipment, applications, or data.
  - The document also includes a list of Security Requirements that must be included in every project requiring a physical or logical access to MIC1 infrastructure, in order to ensure a secure access and to protect MIC1 assets.
- 

## 2. Abbreviations and definitions

- **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 as well people under direct contact with the Contractor (like employees, interims, students, consultants) than any person employed directly or indirectly by the Contractor's sub-contractors.
- **SSLM:** Supervision and Service Level Management
- **Strong password:** a password compliant with following rules:
  - At least eight characters consisting of three from the following combination should be used:
  - 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.
- **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.

### 3. General Terms:

This part details the security requirements, and associated liabilities related to the access (whatever physical or logical) by the Contractor to MIC1 information, applications and systems, as well as related to the delivery of IT/Technology solutions and services by the Contractor to MIC1.

1. The Contractor must ensure at any time strict compliance to all here described requirements.
2. Failure to comply with the below requirements hold the contractor responsible of any loss and/or damage resulted
3. It is the Contractor's responsibility to ensure that all its collaborators are informed of this contract schedule terms and requirements, and that they fully comply with them as well.
4. MIC1 reserves itself the right to verify, maximum twice a year, the compliance of the Contractor with the security requirements expressed in this document, according to the following method:
  - a. If available, the contractor can provide MIC1 with the report of its last security audit conducted by an external independent auditing company.
  - b. If such report is not available, cannot be disclosed, or is judged as non-satisfactory by MIC1, then if needed, MIC1 can request a specific security audit of the Contractor. This audit, executed at MIC1 charge, will have to be realizable at the latest within ten (10) working days after Contractor's receipt of MIC1's request and will be performed by an independent security auditing company, agreed by both parties, and who is not a direct competitor of the Contractor. The Contractor will grant this accredited auditor access to any area, equipment, document or information in relation with the Contractor's mission for MIC1. The auditor will prepare an audit report and present this to both MIC1 and the Contractor. Parties will decide amongst each other on a reasonable grace period during which Contractor will have the possibility to fix reported shortcomings. MIC1 shall have the right to request a check-up audit after this grace period which will not be accounted as an audit for purposes of the "twice a year" possibility to perform an audit.
  - c. Check of the contractor's PCs in case they have onsite presence
5. If, at any time and for any reason, the security requirements are not met, MIC1 shall notify the Contractor and the Contractor shall have a grace period of duration decided on common agreement approximately in the range of 6 months, to cure such situation. If short comings are not fixed after this period, MIC1 reserves the right to close the Contractor's physical and logical accesses to its systems and premises.
6. MIC1 reserves the right, to temporarily suspend, after notification to the Contractor, the Contractor's logical accesses in case that the Contractor's equipment is compromised and represents a direct major security risk for MIC1 (for instance in case of viral infection, data theft, data losses, data corruptions or external intrusion on the Contractor's equipment).
7. All equipment provided by MIC1 to the Contractor and to its collaborators (e.g.: Security ID cards, SIM Cards, tokens, networking equipment, and workstations) remains the property of MIC1 and have to be returned upon completion or termination of this contractual relationship.
8. The Contractor is responsible to take appropriate actions to protect MIC1 equipment provided to him and his collaborators against theft, loss and degradation.
9. The Contractor should take all appropriate actions to prevent Contractor's equipment and solutions, sub-contractors' equipment, and Contractor's collaborators to cause damage, whatever physical or logical, to MIC1 assets (including network, hardware, software, data and brand image). This includes data losses, data corruptions and services interruptions due to:
  - a. Misconfigurations, errors, misconduct, false-operations and voluntary data alterations.
  - b. Spreading of viruses, Trojans, backdoors, or any other type of malicious code, that could happen by Contractor's collaborators, Contractor's equipment and solutions or Contractor's sub-contractors equipment (such as workstations, servers and networking equipment).
  - c. Software running on Contractor's or Contractor's sub-contractors equipment (such as workstations, servers and networking equipment) and disturbing MIC1 infrastructure normal operations.
  - d. Usage of insecure communication link/protocol between their equipments/solutions.
  - e. Non-compliance with MIC1 password policy in particular the Non-compliance with:
    - i. The use of Strong password.
    - ii. Hardcoded password, enabling default username/password, sharing the password with business unrelated persons or setting the password to "Never Expire" are prohibited
    - iii. All System level passwords such as root, windows and applications administrators must be changed on at least quarterly basis and all other accounts on monthly basis
    - iv. Password shall be always communicated in a secure way.

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 could be put at disposal by MIC1 to Contractor's collaborators. MIC1 has the right to suspend the access if any kind of misuse is detected.

#### **4. Physical Access:**

The below guidelines 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 have to be individually and formally registered through the following procedure:

1. Contractor has to send to MIC1, the list of all collaborators who will need access to MIC1 premises. For each collaborator, several information is required: Surname & first name and degree of access frequency (i.e.: everyday, once per week, in backup of somebody...).
- a. Case 1 – For those who regularly access MIC1 premises more than 3 months: Each person pre-identified (as described above) will receive a temporary access card allowing him access to specified areas as per his job requirements. The request will be approved by the administration department (or security department when applicable) after being issued by the head of the concerned department and approved by the respective Sr. HoD.
  - b. Case 2 – For those coming occasionally: Each person pre-identified (as described above) needs to present to MIC1 reception agent upon each visit his identity national card or passport and receives a visitor badge. When the person leaves MIC1 building, he receives back his identity national card or passport, as the badge is returned. The Contractor Collaborator should be escorted in MIC1 premises by the MIC1 team member from the reception to his office or meeting room then back to the reception after the visit is finished.
2. Any person who has been issued a badge must wear it in any plain view at any time. The badge must 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 has to immediately report lost badge.
3. At the end of the contract or when a person's presence is no longer required at MIC1 premises, all security access badges has to be returned at MIC1 reception.
4. For business visits after working hours, a written permission from the MIC1 Contact person's manager and the administration department (or security department when applicable) is required. This written permission will be issued by MIC1 contact person, and will be available with the administration department (or security department when applicable)
5. All the pre-mentioned regulations are applied in all MIC1 locations (Parallel Tower, Libatel, Palm & Pine, Justice, Sin El Fil centers as well as all PoS and PoP) in addition to extra measures depending on the nature of each location which are clarified hereafter

#### **Switches:**

This part of the document is addressed to Contractors who need to access MIC1 switches and datacenters:

1. A list of all collaborators names that will need to enter the switch should be provided by the contractors and signed by the correspondent Sr. HoD at MIC1, who will make sure to distribute it to the administration department (or security department when applicable), who in turn will be responsible to get CTO approval to permit access. The list should include the time and duration of the non-MIC1 employees' missions and should be updated every 3 months; in case of any modification, the administration department (or security department when applicable) should be notified immediately. To note that contractors' interventions on site (day & night) should always be performed in the presence of MIC1 personnel.

2. In case it's necessary for someone outside the list to access the switch, the concerned engineer from MIC1 should send an e-mail to the administration department (or security department when applicable) and copy the concerned Sr. head of department including the full name of who needs to access as well as the date and time duration, then the correspondent Sr. head of department should confirm the request by e-mail or by phone if he was out of office but an e-mail confirmation should be sent ASAP.
3. In case the request was done during non-working hours, the requestor from MIC1 side should call the administration department (or security department when applicable) team to facilitate the mission and who in turn will send an e-mail to the correspondent Sr. head of department to confirm ASAP.
4. It's forbidden to keep inflammable materials inside the switches.
5. Contractor's collaborators should use no doors other than the main entrance doors.
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 to the security department as well as the environment unit ahead of time to take the necessary precautions.

#### External sites of MIC1 network:

This part of the document is addressed to Contractors who need to access MIC1 Network external sites:

1. Contractors' employees must show their company IDs and National IDs to the local guard and write down their data and the task in the log book as well as the guard book.(where applicable)
2. The Contractors' employees must ensure that the shelter and the fence doors are closed well before leaving the site. They should also leave the site clean (they should make sure not to leave any flammable materials or unused items). Every person should call the network surveillance team on 03391313 before entering the site and when leaving the site in order to update the site access database.
3. No one is allowed take any item out of the site without having the pre-approval of MIC1 administration department (or security department when applicable) through an e-mail received from MIC1 contact person.
4. Site must be opened with its key . It's not allowed to try to break the lock or to climb the fence for whatever reason.
5. The Contractor should provide the MIC1 project manager or contact person with a list having all the names of the contractor's employees who need to access the sites as well as their phone numbers.
6. MIC1 NOC maintains and follows up the regular maintenance plans' dates and timings as well as the name of the performing company). In case the contractor needs to access a site to perform regular maintenance procedure in a different time than the one that was previously planned or in case of sudden and unplanned work orders, the contractor should notify NOC team and provide them with the names of who will access,. (i.e.: MIC1 NOC hotline number for the Contractor to use: 03391313)
7. Contractors should be careful in refilling diesel tanks and any leakage should be cleared on the spot.

## 5. Logical Access:

Clauses in this paragraph apply only when Contractor must access MIC1 systems, applications or data, whatever locally, i.e. from MIC1 premises, or remotely, i.e. from any non-MIC1 location.

1. Any information hosted on MIC1 systems, must be considered as confidential, and as such covered by the terms of this document confidentiality clauses. In all cases, this information remains MIC1 property.
2. The Contractor's collaborators will be given a temporary password – valid for one time access – to be changed after intervention completion.
3. All logical access identification media – when applicable - (including logins, Secure ID cards, soft tokens, authentication keys) provided to the Contractor must be used at least once every 3 month. Every one of these media not used at least at this frequency can be automatically disabled without prior notification to the Contractor, and this without any prejudice for MIC1.
4. The Contractors' collaborators will 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 that Internet access filtering to non-ethical sites is applicable inside MIC1. Non-ethical site meaning (without being restricted to) all content that may present a risk for MIC1 or which distribution may constitute an infringement to laws, specifically laws against harassment and racism.

- b. They will comply with the access rights provided to them by MIC1, and they will never try to execute actions which would bypass these provided access rights.
  - c. They will never execute actions (like install or use of software) that would infringe software licensing policies or violate digital property regulations.
5. Unless this is especially required for executing the mission described in this contract's scope, Contractors' collaborators will never, without prior written permission from their MIC1 technical contact:
  - a. Change any access rights, or create users' accounts, on the accessed systems or applications.
  - b. Profit from granted privilege or proprietary data that could reside on MIC1 systems.
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) will 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 and establishing direct or indirect connections to the MIC1 network (including users' workstations, servers, routers) will (if applicable):
  - a. Be in order of licenses for all software installed on it.
  - b. Be physically and logically protected from use by other people than MIC1's or Contractor's collaborators.
  - c. Be properly configured and secured according to the state of art of IT security.
  - d. Not run any software that could interfere with MIC1 infrastructure. Typically:
    - Workstations must be equipped with up-to-date anti-virus and personal firewall or personal intrusion detection software,
    - Servers and workstations access must be protected using strong password
    - Servers and workstations directly communicating with MIC1 private network won't run any network information service or network dynamic configuration service that could interfere with MIC1 similar services (like DHCP, DNS, WINS or dynamic routing information services)

- Servers and workstations directly communicating with MIC1 private network won't run application putting at stake MIC1 equipment (like network scanners or, vulnerability detection software).
  - e. Use secure connection
8. If the Contractor detects any security exposure, misuse or non-compliance situation, he should contact MIC1 contact person who in turn should contact the ITI department (or security department when applicable).
  9. If the Contractor notices the loss or theft of any provided MIC1 asset then he should contact MIC1 contact person who will in turn contact the security hot line.  
(MIC1 Security hotline: +961 3 391112)
  10. The Contractor commits itself not to use the provided accesses to get information about MIC1's business, customers or partners, which wouldn't enter the scope of the mission expressed in this contract. Typically, the Contractor will never tap communications that MIC1 would have internally or with its other contractors, partners or customers.
  11. All connection sessions to MIC1 network, equipment and applications may be monitored and logged by MIC1. The Contractor is informed that these log records can be used to enforce a claim brought by MIC1 against the Contractor for not having complied with its obligations. Should such log records be used as evidence, the Contractor shall be allowed to have access to them in order to assess the case.
  12. Upon contractual relationship termination, the Contractor will return to MIC1 any data put at his disposal that are MIC1 property (including databases copies, project information files, etc.), and definitively wipe out any copy of these data stored on its equipment (including workstations, servers and backup devices).

## **6. Local Access:**

Clauses in this paragraph apply only when the Contractors' collaborators act inside MIC1 Premises (whatever office spaces or technical sites).

1. The Contractor's collaborators will never connect any equipment non-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 shall be performed through an MIC1 owned workstation
3. In the event that such non-MIC1 equipment is authorized for being connected to MIC1 private data network, this equipment must be:
  - a. Registered with the MIC1 Service Desk via a Request For Change
  - b. Equipped with an up-to-date anti-virus and operating system.
  - c. Protected from theft by the contractor
  - d. scanned for viruses and vulnerabilities, by the DMS (Desktop and Microsoft Support) unit for approval to be connected to the WLAN and LAN .A certified up to date anti-virus should be installed on that laptop, latest OS patches should be installed and no vulnerabilities should be present
3. The Contractors' collaborators will comply with all MIC1 InformationSecurity Policies published on MIC1 intranet web site and available on request.
4. Visitors/consultants who need to access only e-mail and Internet should use the wired/wireless guest VLANs
5. When connected to the MIC1 WLAN, no bridging is allowed such as wired and wireless access. The Contractor collaborators should never use any tunnelling software, providing access to any external network. ITI department (or security department when applicable) will have the right to block any such connectivity when discovered



## 7. Remote Access: Networks Interconnection

Clauses in this chapter apply only when a network interconnection must be established between MIC1 and the Contractor's (or subcontractor's) networks. This interconnection can be intended as well for accessing MIC1 internal applications and systems from remote location.

- a. .
- Contractor's network and devices, which are directly or indirectly connected to the MIC1 network, cannot have any non-filtered network connections to any third party networks or equipment (for instance the Internet or another private network). "Filtered" means here "at least controlled by properly managed firewall equipment".
- The Contractor will strictly restrict the accesses to its equipment directly or indirectly connected to MIC1 network. Only the people required for fulfilling this contract's mission can be allowed to connect to this Contractor's equipment.
- The Contractor (and Contractor's collaborators) will 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 (as VPN gateways, firewalls routers...). Under no circumstances can these ones be written down visibly on devices.
- For interactive accesses, the Contractor's collaborator will always disconnect from the MIC1 target systems after job achievement, as system will disconnect after 10 minutes of no activity.
- MIC1 will take all reasonable measures to prevent any unauthorized access to the Contractor network through the interconnection. The Contractor is also responsible to take all reasonable measures to protect its IT infrastructure from illegitimate accesses.
- Under any condition, dial up connections are not allowed at all to Internal MIC1 systems.

## 8. Network, Systems and Solutions

General Requirements:

Following requirements apply for all contracts of IT and Network solutions development, delivery, installation, support, and operation.

1. The Contractor must comply with MIC1 Change Management process. This process is available upon request. Practically, it means that any intervention intended at changing an equipment hardware, software or configuration must be prior communicated to the MIC1 technical contact, in order for him to create a change request ticket in the MIC1 change management system. It's only after validation of this request by impacted teams that the intervention can be executed. Requests shall be sent 48hours prior to any change for proper assessment and approvals.
2. The Contractor will request from its MIC1 correspondent an explicit written authorization prior executing any change that would lower the security level of the equipment and/or service related to this contract's scope, or of any other MIC1 equipment or service. It's the MIC1 correspondent responsibility to evaluate this change in agreement with MIC1 security team.
3. Every intervention, whatever planned or executed in emergency, must result in an intervention report that will be sent by e-mail to the MIC1 technical contact person who will in turn follow the right process. This report must 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 to the Contractor as a result of executing this contract (as for instance dump files, database extracts, etc.):
  - a. Can be used only in the scope of this contract's mission.

- b. Will be kept only for the strict duration of the required intervention, and will be definitively destroyed by the Contractor afterward.
- c. Will be considered as confidential, and as such protected by this contract's confidentiality clauses.

Moved systems: In the case that the contractor would have to move MIC1 systems outside MIC1 premises in order to execute its mission, The Contractor must ensure that all systems moved outside MIC1 premises are properly covered by an insurance contract as long as they are under the responsibility of the Contractor. This insurance contract must cover any losses, including theft, physical and logical damage (as for instance data losses or corruption).

The Contractor is exceptionally allowed to take a copy of the data and software hosted on the moved systems for backup purposes during the intervention. Normally, these backups must be stored in a safe place at MIC1 premises and protected from unauthorized access. All these backup copies must be erased after that the MIC1 technical contact has confirmed that the systems have been moved back to MIC1 premises and that requirement to provide backups is over. Providing backups to contractors should follow an exceptional & abnormal approvals flow. Contractors should commit on not offering/installing/utilizing any equipment which can cause security threat or information leakage that jeopardizes MIC1 network security.

- 5. All vendors, contractors, sub-contractors are forbidden from taking photos inside MIC1 critical sites and premises, unless approved by MIC1
- 6. When applicable, to prevent any 3rd party Laptop to be directly connected to MIC1 network, from having administrator' rights
- 7. All Solutions offered by the supplier should at least comply with the following requirements to ensure that it is secure and that it will not jeopardize MIC1 environment:
  - Application should run without the need of root (unix) admin (win) privileges
  - Applications shall support installation of an Antivirus and its updates
  - OS, Database and Application admin users should be separated
  - Systems shall support patching mechanism in a way that Contactor (upon MIC1 request) or MIC1 deploys the most recent security patches without interfering with the applications and within a timeframe set by MIC1
  - Solutions shall comply with MIC1 Password policy in particular:
    - The use of Strong password.
    - Hardcoded password, enabling default username/password, sharing the password with business unrelated persons or setting the password to "Never Expire" are prohibited
    - All System level passwords such as root, windows and applications administrators must be changed on at least quarterly basis and all other accounts on monthly basis
    - Password shall be always communicated in a secure way.

Failure to comply with the above requirements holds the supplier/contractor fully responsible of any malware ( virus, worms, Trojan , botnet) spread resulting in damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on MIC1 data, hosts, or networks

If investigations show that the source of the network malware is from any of the systems and solutions Supplied by the contractor then the contractor shall take prompt actions in cooperating with MIC1 team to remove the malware and pay the indemnities for the caused damages that will be assessed after the incident.

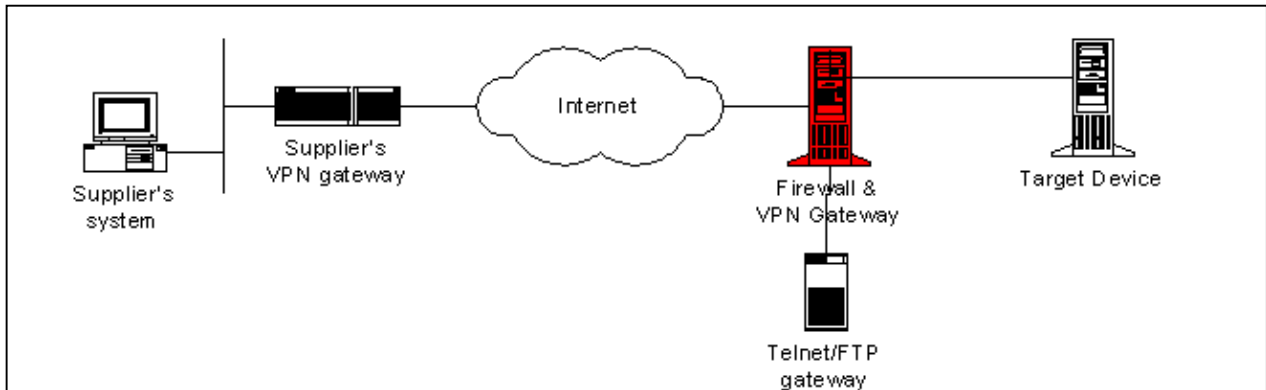
## 9. Remote Networks Connectivity

The networks connectivity is the technical setup realized in order to allow the Contractor's systems or collaborators located outside MIC1 premises to communicate with MIC1 equipment. This can be on-demand connection, activated only upon request. Such remote connectivity is not approved for suppliers that have a local presence in Lebanon as they should perform all activity on the systems on site. All initial installations should be done by the suppliers on site even if he hasn't got any local presence, Remote connection could be allowed after acceptance issuance and for support purposes.

The only approved method of remote connectivity is the “LAN-To-LAN IP VPN over Internet” which can be described in the below schema.

MIC1 Template for connections requirements should be filled by both parties before establishing any connection.

Connection Architecture:



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