وزارة الاقتـــصاد
الرقمـي والريادة

Heading
Document name: Supply Chain Security Policy
Document number: MODEEP-18

Service recipient
Internal: E-Government
External: None

Document owner: Information Security Directorate

Document Control
Version number: 1.0
Release Date: 14/08/2023
Final approval: Information Security Director

Document Versions:

Version	Date	Notes
V1	**18/4/2023**	First Release

1.1. Objectives

The purpose of this policy is to ensure that all contracts and dealings between ministry of Digital Economy and Entrepreneurship (**MODEE**) and third-party suppliers have acceptable levels of information security agreement to protect personal and business data.

1.2. Scope

This policy applies to all third party who worked or aimed to work with MODEE.

1.3. Policy Terms

1.3.1. Security Third Party Agreement

1. Third party access to MODEE.'s information systems shall be granted based on a formal contract between MODEE and the third party.
2. All third-party agreements shall be consistent in all respects with MODEE information security policies, procedures, standards, and guidelines.
3. Contracts with third parties for provision of third parties with access to information systems shall be consistent in all respects with MoDEE according to information security policies and procedures. In addition, third parties shall be required to follow the same procedure for granting and revoking third party access to MODEE Information Systems Infrastructure which is followed for granting such access to MODEE employees.
4. Third party contracts shall include the following conditions as a minimum:
   - Provision for confidentiality, non-disclosure and acceptable use relating to the information / data accessed or processed by the outsourced function or service.
   - Penalties to noncompliance with security level agreement should be defined.
   - Compliance with legal and regulatory requirements.
   - Compliance with Intellectual property rights requirements.
   - Compliance with MODEE. information security policies and procedures.
   - Clear allocation of responsibilities to all the involved parties.
   - Statement on Non – Disclosure of information.
   - MODEE rights to review and audit the compliance with the contracts.

- ➢ All External Parties.
- ➢ SLA, as applicable.

5. In case of outsourcing information or data processing functions or services to third party organizations, the supplier should make sure that the 3rd party comply with MoDEE's security requirements.
6. Standard procedures must be documented and approved to manage the relationship between MODEE and third party before, during and after the termination of the contractual relationship.

1.3.2. Supplier Selection

1. Proposals and suppliers' provided solutions shall be exercised while evaluating suppliers' services to ensure accuracy of their claimed qualifications and successful delivery of contractual obligations.
2. Project Managers or legal department shall ensure that contractual agreements in terms of legal, business, and technical requirements is negotiated and agreed with the External Parties, before exchanging any information, as per the contractual obligations.

1.3.3. Outsourcing or managed services

1. To obtain information technology support or managed services, the third party must be carefully selected, and the following must be verified:
   - ➢ Cybersecurity services operations centers managed for operation and monitoring that use the remote access method must be located entirely within Jordan.
   - ➢ Outsourcing penetration testing on sensitive systems must be provided by national companies, entities and individuals, in accordance with the relevant legislative and regulatory requirements
   - ➢ Security scanning shall be conducted for outsourcing companies, outsourcing personnel, and managed services working on sensitive systems.

1.3.4. Identification of Risks related to External Parties

1. Any Project Manager in coordination with information security section shall identify any additional information security risk specific to the project.

2. The analysis of risks related to External Parties access to information and information processing facilities shall consider the following:
    a. Possible impacts on the controls of the information processing facilities.
    b. The classification of the information assets.
    c. Processes for identifying, authenticating, authorizing, and reviewing access rights of the External Parties.
    d. Security controls that are in place to control storing, processing, communicating, sharing, or exchanging information.
3. All risks identified shall be appropriately addressed through risks mitigation measures.

1.3.5. External Parties Access Management

1. The External Parties shall be provided access to information & information processing facilities as per the Access Control Policy.
2. The External Parties shall be provided access to information & information processing facilities on the principles of need-to-know basis.
3. The provisioning of External Parties access to information & information processing facilities shall be granted on temporary basis. Wherever feasible, this access shall be configured with specific end date so that it gets expired at the end of the contract.
4. The usage of managed laptops by the External Parties shall be based on approval from information security section.
5. External Parties shall not be granted with remote access before obtaining prior approval from system owner, and in this case, no VPN is allowed.
6. Remote access of third parties shall be through conference supervised by MoDEE system/network admin.
7. Controls related to passwords shall be applied to all users who have access to information of MODEE. in line with the cyber security requirements and objectives
8. Multi-factor authentication system should be applied to access sensitive systems that process, transmit, or store information for MODEE.
9. access rights should be periodically reviewed in accordance with the approved cyber security policies.

10. All audit records shall be stored, maintained and made available upon the request.

1.3.6. Information protection requirements

1. Third parties must process, store and destroy the information of MODEE. in accordance with the "سياسة استخدام موارد تكنولوجيا المعلومات" in MODEE..
2. Appropriate encryption controls must be applied to protect the data and information of MODEE and to ensure that its confidentiality, integrity and availability are preserved in accordance with the encryption standard approved by MODEE.
3. Back-up copies of the data and information of MODEE must be made periodically and in accordance with the backup management policy of MODEE.
4. The data and information of the MODEE in sensitive systems must be classified.
5. Respective Projects Managers shall maintain appropriate reports and records, to monitor and measure the compliance with the information security requirements. The External Parties shall be responsible to take appropriate actions to address any non-conformity may be identified during the compliance review.
6. Security events logging shall be fully activated for all information processing facilities to which access is provided to External Parties as per the contractual obligations.

1.3.7. Cybersecurity incident management and business continuity

1. The terms of contracts and agreements with third parties must include requirements related to reporting cybersecurity incidents and informing MODEE in the event that the third party is exposed to a cybersecurity incident.
2. Communication procedures between the external party and MODEE must be defined and documented in the event that the external party is exposed to a cybersecurity incident, and these procedures must be reviewed and updated periodically.
3. An appropriate business continuity plan must be developed to avoid unavailability of services provided to MODEE. in accordance with the requirements of the business continuity and disaster recovery plan for MODEE.

1.3.8. Termination of External Parties services

1. Upon completion/termination of an engagement with External Parties, Project owner shall inform the relevant Administrator to revoke the access rights of the External Parties that was granted to information processing facilities.
2. Project manager shall ensure that proper transfer of knowledge is obtained from the External Parties for the ongoing operation / maintenance.
3. Project manager shall ensure that all MODEE assets provided to the External Parties are returned such as laptops, books, manuals, documentation, building keys, magnetic access cards etc.
4. Any connections between the External Parties' network and MODEE network shall be terminated in cases of any security breach that may occur or non-compliance of the External parties to any Customer policies.

1.4. Associated Processes and KPIs

1.a Information security section should establish a process to annually review the existent agreements with third parties to check for security requirements.

1.5. Roles and Responsibilities

1. Policy Development and compliance: information security section
2. Policy Review and Approval: information security section
3. Policy Implementation and adherence: Tendering unit, PMs, OPS, Legal Dept, information security section.

1.6. Compliance

Compliance with this policy is mandatory. **MODEE** management must ensure continuous compliance monitoring within their departments. Compliance with the statements of this policy.