

THIRD PARTY INFORMATION SECURITY POLICY

A risk assessment should be made before granting access to AROMSA information systems to employees of third parties. The following criteria should be considered when granting access to third parties.

Third party employee or company representative informs the information system he/she wants to have access to.

- Access method (physical access, logical access, access from or outside of AROMSA) should be determined as described in the Security Policy (BGYS.POLTK.02) and *Access Control Procedure* (SÇP.28).
- Importance and value of the information to be accessed should be determined by the System/Asset Owner.
- The Level of audit logs for third party employees' access to AROMSA information systems should be determined by the IT System Manager and IT Business Application manager.
- Necessary measures to protect the information that is not open to access of third parties are described in *Access Control Procedure* (SÇP.28) and necessary references are made to this Procedure.
- Legal requirements and contractual obligations of parties other than AROMSA should be taken into consideration.

In the event of changes in purchasing of services including protection and improvement of available information security policies and procedures (information Security Management System Policy -BGYS.POLTK, Access Control Procedure (SÇP.28), Physical Security Policy - BGYS.POLTK.02, Human Resources Safety Policy- BGYS.POLTK.03, Network Safety Policy- BGYS.POLTK.06, Information Exchange Policy - BGYS.POLTK.08, Record Management Policy- BGYS.POLTK.09, information security Breach Management Procedure- SÇP.29, Version Update and Patch Procedure- SÇP.32, Adaptation and Software Development Procedure- SÇP.37) and instructions (ABAP Standards INstruction-KT.BG.003) , risks involving third parties should be reviewed by asset owners and information security Manager. Change requests can come from AROMSA and third parties.

The following should be taken into consideration when managing changes in third party agreements:

1.1 Changes that can be made by AROMSA

- Improvements on existing services,
- Development of new applications and systems,

- Changes or updates on organization policies and procedures,
- New checks and controls to solve information security events and improve safety.

1.2 Changes that can be made by third parties;

- Changes and improvements on networks,
- Use of new technologies,
- Acceptance of new products or final versions,
- New development tools or media,
- Physical location change for services,
- Change of manufacturing company.

Changes made are included in supplemental agreements.

Without an agreement with a confidentiality clause or a separate confidentiality agreement, no access to sensitive information should be granted to third party employees. Relevant policies and procedures are referenced in such agreements or confidentiality agreements.

If a third party requests to connect a system to AROMSA network, then the third party should act in accordance with AROMSA information security policies. This is necessary to ensure and maintain protection against malware.

Third party companies that are granted access to AROMSA information systems should have a contact person with whom safety issues can be discussed.

Access of third party employees to AROMSA network and systems should be limited to their duties described in service agreements. If third party employees need to have access to AROMSA systems / applications to do their work, they should comply with the Access Control Procedure (SCP.28) and other relevant information security policies.

When adding users in the company systems, project and agreement terms are checked for third party employees. Upon the termination of a contract/agreement, user access is automatically denied. During periodical review of access rights, access rights granted to third parties are also reviewed.

All third party access permits are periodically reviewed and removed when they are no longer necessary.

Service providers, services or products are checked for compliance with relevant agreements during acceptance inspections of third party services and/or products.

A legal procedure is initiated for products or services that fail at acceptance inspection. If necessary, claims for damages/losses are made.

2 Handling of information security in Third Party Agreements

The following terms and conditions should be included in agreements to meet safety requirements.

2.1 Reference to AROMSA Information Security Policy

2.2 Measures for protection of assets.

For example,

- Procedures to protect the company's assets including information, software and hardware,
- Necessary physical security measures and mechanisms,
- Safety measures against malware,
- Procedures to understand whether there is any danger for assets (loss or change of information, software and hardware),
- Measures to ensure return or destroy of information when an agreement is expired or at a specified time when the agreement is still valid,
- Confidentiality, integrity, availability (accessibility) and other asset properties,
- Limitations concerning reproduction and disclosure of information and use of confidentiality agreements,
- A clearly understandable reporting structure and agreed reporting format if necessary,
- A clearly understandable and well-defined information exchange management if necessary,
- Provisions on employee transfer if required.

2.3 If necessary details and clauses about access of third party employees to AROMSA information systems are added as supplemental clauses into agreements.

- Third party employees should comply with AROMSA's security and safety policies, standards and relevant laws and regulations,
- Safety obligations of third parties should be clearly defined,
- AROMSA is entitled to monitor the access of third parties to AROMSA information systems and prevent this access on its own discretion,
- Necessary confidentiality agreements should be in place to ensure and protect intellectual rights, patent rights, joint effort products/outcomes ,
- AROMSA's information assets should be taken back or destroyed after an agreement is terminated,
- Access to AROMSA information assets should be cancelled when an agreement is terminated.

Third parties should first consult to AROMSA before making any decision to use subcontractors for any service provided to AROMSA and should never employ subcontractors without AROMSA's approval.

Third parties are periodically monitored and reviewed. Third parties providing service to the company can be inspected according to the annual supplier inspection plan for information security.