



Confidentiality Policy

This confidentiality policy explains how Rees Mobile Services Ltd expects our employees to treat confidential information. Employees will unavoidably receive and handle personal and private information about clients, employees, and our company. We want to make sure that this information is well-protected.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive customer data)
- Constitute the backbone of our business, giving us a competitive advantage (e.g. business processes)

Scope

This policy affects all employees who may have access to confidential information.

Policy elements

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated. Common examples of confidential information are:

- Unpublished financial information
- Data of customers/employees
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Employees may have various levels of authorized access to confidential information.

Employees who have access to Rees Mobile Services Ltd.'s confidential information should:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure they only view confidential information on secure devices
- Only disclose information to other employees when it's authorized, necessary and in a confidential area
- Keep confidential documents inside our company's premises unless it's absolutely necessary to move them

Employees should not:

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of our company (e.g. family members, friends, acquaintances, other business')
- Replicate confidential documents and files and store them on insecure devices

Should an employee stop working for Rees Mobile Services Ltd, they're obligated to return any confidential files and delete them from their personal devices. If requested, employees shall also disclose all passwords linked to Rees Mobile accounts or documents upon termination. Management will require proof that this step has been completed.

Confidentiality measures

Rees Mobile Services Ltd will take measures to ensure that confidential information is well protected.

We'll:

- Store and lock paper documents
- Encrypt electronic information and safeguard databases
- Ask employees to sign non-disclosure agreements
- Ask for authorization by senior management to allow employees to access certain confidential information

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons.

Examples are:

- If a regulatory body request's it as part of an investigation or audit
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, employees involved should document their disclosure procedure and collect all needed authorizations. Rees Mobile Services Ltd. is bound to avoid disclosing more information than needed.

Disciplinary consequences

Employees who do not respect our confidentiality policy will face disciplinary action and, possibly, legal action.

Rees Mobile Services Ltd. will investigate every breach of this policy. We will terminate any employee who willfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to punish any unintentional breach of this policy depending on its frequency and seriousness. We will terminate employees who repeatedly disregard this policy, even when they do so unintentionally.

Note: This policy is binding even after separation of employment.

Employee Signature

Date

Employee Name (Print)

Employee Job Title