1. Aim

This Policy defines the rules applied for internet users within MAUN.

2. Scope

All users within MAUN are covered by this policy.

3. Responsible

The administration is responsible for establishing this policy. All MAUN internet users are responsible for the implementation of the policy.

4. Rules

If the senior management deems it appropriate, internet access over the corporate network can be monitored without notice under the KVK (Personal Data Protection) Law. Users must act with this awareness.

The internet within MAUN cannot be used for the following purposes:

- Sending unsolicited messages (SPAM messages) such as commercial advertisements and news announcements,
- Using another user's e-mail account for the purpose of sending messages without the express consent of that user,
- Production and distribution of offensive material that does not comply with the intended use (except for academic and research purposes),
- Production and distribution of material that is unrealistic, distressing and disturbing, and that creates unnecessary fear,
- Production and distribution of slanderous and defamatory material,
- Distribution of copyrighted material (including but not limited to articles, articles, books, films, musical works) that violates the intellectual rights of others,
- To carry out all kinds of work and transactions that will leave the institution or individuals in a difficult situation legally,
- The following types of applications made on purpose;

- Destroying other people's data,
- Infringing on the personal information of others,
- To disrupt, destroy the works of others,
- Creating traffic that will not allow others to use it,
- Persistently using software that is prohibited by the administration because it prevents the institution from working, causes risky situations and creates unnecessary traffic.

5. Sanction

In case of violation of this policy, the reason for the violation is investigated by obtaining the necessary personnel support by the Administration. Violation is unintentional and personnel training, etc. If it is caused by a deficiency, work is done to close the deficiency that is the source of the problem. Personnel are warned in writing via e-mail.

If the violation is understood to be intentional or if the unintentional violations are repeated more than 3 times, action is taken against the personnel in accordance with the civil servants law no. 657 and the additional sanctions specified in the official letter of the University.

All users are responsible for reporting incidents of security breaches and violations of this policy to the Administration as soon as possible.