	E-MAIL USAGE POLICY	Document number	MSU.BG.PL.03
		Release date	05.03.2021
		Revision Number	
		Revision date	--
		Page Number	1/3

1. Aim

To define the rules for personal and business use of MŞÜ e-mails.

2. Scope

Within the scope of this policy, the principles regarding the use of e-mail addresses within MŞÜ are discussed.

3. Responsible

The administration is responsible for establishing this policy. All personnel are responsible for the implementation of the procedure.

4. Application

E-mail is one of the most important communication channels of a business and it is inevitable to use this channel.

Unauthorized Usage Methods of E-Mail System

- The e-mail address officially allocated to the user cannot be used for malicious and personal benefit.
- The e-mail system of the institution cannot be used to send messages such as spam (junk e-mail), phishing (phishing) to other internal and external users.
- Any internal or external user and group; defamatory, insulting and damaging e-mail messages cannot be sent.
- If messages are to be published on internet newsgroups, the official e-mail address provided by the institution cannot be used in these messages. However, the official e-mail address provided by the institution can be used, with the approval of the manager, for internet news groups that are useful to be a member of for business purposes.
- No user can write the e-mail address of another user in the from section of the e-mail address he sent without his authorization.
- Staff SUBJECT field should not send an empty email message.
- The SUBJECT field is blank and should be deleted without opening any anonymous e-mails.

- File extensions to be attached to the email cannot be ".exe", ".vbs" or other prohibited extensions. In cases where such files must be transmitted, the files will be compressed (in zip and/or rar format) and added to the message.

- User accounts must not be used directly or indirectly for commercial or profit purposes. Emails should not be sent to other users for this purpose.

Prepared	controlling	approver
EFRAİM YILDIZ	CENGİZ ALMAZ	İHSAN TUĞAL

- The institution's e-mail system cannot be used to send messages that contain elements of harassment, abuse, or in any way illegal to harm the rights of the recipient. When a message with such characteristics is received, MŞÜ CC should be notified immediately.

- In order for the messages not to reach anyone other than the person they are sent to, maximum attention should be paid to the address sent and the information it contains.

- No confidential information can be included in messages within the scope of information security. This includes the items embedded in it.

- Chain messages (spam), any executable files attached to messages, any e-mails containing harmful links attached to messages should be deleted immediately when received and should never be forwarded to others.

- Chain email, fake email, etc. Harmful e-mails should not be replied to or shared.

- Inappropriate content (racism, political propaganda, material containing intellectual property, etc.) should not be sent in the e-mail.

- The user accepts that all expressions expressed during the use of e-mail belong to him. The user is responsible for the content of messages that may constitute a crime, threatening, illegal, insulting, abusive or slanderous, immoral.

- Personnel should not use their personal e-mail accounts (eg gmail, hotmail, yahoo, mynet etc.) in their business correspondence.

- Staff should prevent their messages from being read by unauthorized persons. Therefore, a password should be used and the hardware/software systems used for e-mail access should protect against unauthorized access. Computer or mobile devices must have a screen protection password.

- If the personnel working in the field access their corporate e-mails from mobile devices, they must ensure the confidentiality of the information and at the same time, they must use a password on their mobile devices to ensure this confidentiality.

- Considering that the e-mail that asks users to enter a user code/password may be a fake e-mail, it should be deleted immediately without any action.

- E-mail users are responsible for preventing corporate e-mails from being seen and read by outsiders and unauthorized persons. At the same time, the employees of the institution cannot forward their corporate e-mails, together with their contents, to the e-mail accounts of persons outside the institution or unauthorized persons.

- Files in e-mail attachments of unknown origin should never be opened and should be deleted immediately.

Prepared	controlling	approver
EFRAİM YILDIZ	CENGİZ ALMAZ	İHSAN TUĞAL

- The user with an e-mail address is responsible for submitting the Personnel Department dismissal document to the CC via EBYS in cases such as retirement or leaving the job.

- The user must respond to corporate messages in a timely manner so that the corporate workflow is not disrupted.

- The user should not send more than 50 messages per minute via the @alparslan.edu.tr corporate e-mail account. Submissions exceeding 50 per minute will not be forwarded to recipients.

- Files that come as attachments to e-mails of unknown origin should never be opened, and e-mails thought to be a threat should be notified to MŞÜ CC System Management.

- The user is responsible for the security of his e-mail password and the legal actions that may arise from the e-mails sent, and should notify MŞÜ CC System Management as soon as he realizes that his password has been broken. He should change his password immediately.

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 by the university official letter.

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

Prepared	controlling	approver
EFRAİM YILDIZ	CENGİZ ALMAZ	İHSAN TUĞAL