1. PURPOSE

The purpose of this directive to provide the necessary instructive information, for the use of information systems of the Koç University, and determine the limitations and regulations regarding the use of the related systems to prevent the misuse of Information Technologies equipment, and malfunctions and vulnerabilities from emerging on related systems, and data loss, unauthorized access to data and similar risks arising from these malfunctions and vulnerabilities.

2. SCOPE

This directive applies to all KU members, graduates, and all personnel of companies that provide support services to KU, and all users inside or outside of the campus to whom the University grants right of access to Information Systems and Information Technologies services.

3. REFERENCES

3.1 KU Information Security Directive

3.2 KU Password Procedure

3.3 CoHE Student Discipline Directive

3.4 Koç University Administrative Personnel Directive

3.5 Preserving and Destroying Personal Data Directive

3.6 Koç University Ethical Conduct Rules and Application Principles

3.7 Within the scope of COBIT.2019, any one of "Process, Organizational Structures, Information Flow and Entities, People, Skills and Events, Policies and Procedures, Culture, Ethics and Manners, Services, Infrastructure and Applications" governance components that can be applied to the relevant governance and management goal.

3.8 All of the ISO 27000:2018 Information Security management standards family.

3.9 SANS-CIS controls are strings of cyber security actions that provide specific and applicable measures to stop most common and dangerous attacks.

3.10 5651: Law on Regulation of Publications on the Internet and Suppression of Crimes Committed By Means of Such Publications

3.11 6698: Law on the Protection of Personal Data

3.12 4857: Labor Law

3.13 2547: CoHE Law

3.14 5846: Law on Intellectual and Artistic Works

4. RESPONSIBILITES

4.1 The Rector is responsible for the enforcement of this directive.

4.2 The Information Technologies Directorate is responsible for preparing the Directive for publication, enforcement and monitoring the optimization of the Directive.

4.3 The Information Security Committee is responsible for evaluating non-defined situations regarding Information Security and determining the code of practice.

5. DEFINITIONS

5.1 **Directive:** Acceptable Use Directive

5.2 **KU members:** Administrative personnel, academic personnel, students.

5.3 **IT:** Information Technologies

5.4 **Information Systems:** Indicates sources which are owned, rented, adapted, protected, or kept under control by the University; computers, network, cloud, and internet-based services whether be personal or provided by the institution, portable equipment/storing devices, software, and all kinds of hardware, equipment, and intellectual property related to this, within this framework.

5.5 **Information Security Committee:** This is the Supreme Committee which is responsible for mitigating information security risks and providing consultancy in matters of security, determining the security policies, evaluating new threats, and ensuring that regulations such as Law on the Protection of Personal Data are conformed to.

6. FUNDAMENTAL PRINCIPLES

6.1 In the case of violating or causing the violation of this directive and other related directives and procedures, for the KU Administrative personnel Labor Law No. 4857 and Koç University Administrative Personnel Directive will be enforced, for the KU Academic personnel CoHE Law No. 2547 will be enforced and for the students, CoHE Student Discipline Directive will be enforced.

6.2 The University holds all rights over information systems belonging to the University.

6.3 The University only grants a personal, non-transferable, and non-exclusive right of use to users

regarding the use of information systems.

6.4 By using the University's information systems, all users accept the following;

6.4.1 That the University preserves its rights specified in this document and that the use of systems in question is limited to purposes approved by the University,

6.4.2 And that the necessary notifications were made to them in this respect.

6.5 All users are obligated to conform to the related legislation, particularly the "Law on Regulation of Publications on the Internet and Suppression of Crimes Committed By Means of Such Publications no. 5651", and Koç University's Ethical Conduct Rules and Application Principles when using all means of the information systems and communication, including use of internet and vocal communication, and in providing these means.

6.6 All users are obligated to conform to the Law on Intellectual and Artistic Works legislation, for software that may be found in their computers besides standard work and office applications (software besides the operating system, antivirus, office applications, work applications and etc. provided by the University).

6.7 When it is necessary, the University can completely or partly block the access to whole or part of the information systems (for all or some of the users) without giving any notice.

6.8 Users of the University's information systems must conform to the Koç University's Acceptable Use Directive and by using IT systems, they accept that they approve the Acceptable Use Directive and they will conform to it, they were notified in this respect, and that allow the University to apply the Acceptable Use Directive. Users also accept that they will conform to the related legislation and will avoid all kinds of behavior which will put the University under obligation.

6.9 The University preserves its right to change the Koç University's Acceptable Use Directive and other conditions regarding the use of information systems at any time and without giving notice in advance, and its right to take actions which may be necessary or appropriate for conformity with the related legislation.

6.10 The University preserves its right to limit or block someone's use and its right to analyze, copy, remove or change all kinds of data, file or system resource in the information systems belonging to the University, which may damage the use that is deemed appropriate for information systems or may be used to violate the rules or policies of the University, without giving notice in advance; to protect the

University's information systems and the integrity of users against the unauthorized or inappropriate use of the facilities in question and to detect violations of the University's rules and policies and possible use which would cause a violation. Koç University preserves its right regarding the periodic review of the system to protect its information systems and all its rights. Harmful software scans conducted on computers and on servers belonging to the University and e-mails processes in University servers can be given as an example of reviews that will be conducted to protect systems.

6.11   In the event of the user conducting data transfers inside an information system or between information systems via technical means, without logging it in to the systems, for personal reasons, the person's actions and purposes will be inspected. If it is deemed necessary, for the personnel the Human Resources, and for students, the related Diaconate will be informed.

6.12   The University can block access to some websites, keeps a log of information regarding internet traffic, and reports them to official authorities if they are requested by operation of Law no. 5651 (Law on Regulation of Publications on the Internet and Suppression of Crimes Committed By Means of Such Publications)

6.13   All users must ensure that the antivirus software is installed, updated, and works on their computers/phones, and all devices that work by connecting to the Internet or the University's network. If they have questions in this context, they must contact the Information Technologies Directorate. The University may block the e-mail, Intranet, or Internet access of a user who deactivates the antivirus software or who tries to interfere with the antivirus software without authorization.

6.14   Users must be close to the printer when printing a highly classified document to prevent the information from being seen by people without clearance or the information being obtained. Users cannot leave prints of original and copy documents inside printers and photocopiers, whether the documents are classified or not, even if they are stuck in the machine. It is forbidden for documents whose copyright don't belong to the University to be reproduced using printers and photocopiers belonging to the University. The use of printers and photocopiers must be monitored. Their use for non-work purposes and misuse must be evaluated and necessary actions will be taken.

6.15   In the event of a violation of this directive by someone else, an error regarding the security of information systems or all kinds of information regarding the security being bypassed is being detected, it is obligatory for the Koç University's Information Technologies Directorate to be informed of this incident within the scope of the Information Security Incident Management.

6.16   **Terms of Use**

6.16.1   The users cannot copy, change, reproduce, create works derived from, reverse engineer, dismantle or decompile in any other matter, any software, or any other component of the information systems.

6.16.2   Users cannot use information systems that they are not authorized to use and to which the University hasn't granted access to. Unauthorized use of the information systems by obtaining false or deceptive credentials to access information systems or by any other means is forbidden.

6.16.3   Users cannot use the University's information systems to obtain unauthorized access to information systems of other institutions, organizations, or people.

6.16.4   Users cannot authorize anyone to use University accounts for any reason. The account owner is responsible for all kinds of use of the University account. Users must take all reasonable precautions including password protection and document protection to prevent their accounts from being used by unauthorized people. Users cannot share their passwords with anyone within the scope of principles stated in the "Password Procedure", and passwords must be changed regularly. Responsibility for all kinds of processes conducted by using a password of a user account falls on the account owner even if the process was not conducted by the account owner.

6.16.5   Users must not transmit their University address and phone number, e-mail address, and other personal information provided by the University to social media sites on the internet (discussion groups, chat rooms, other forums, etc.) apart from situations where it is required by business or law.

6.16.6   Information systems of the University must only be used in matters related to the University, in a manner permitted by the University. It is forbidden for all information systems of the University, including the campus network, to be used for personal or commercial purposes, apart from situations where it is explicitly allowed. Information systems of the University cannot be used for any illegal purpose, including but not limited to collecting, installing, and distributing software via fraudulently or illegally obtained media files. Use of external networks or services – including cloud services – must be in accordance with the Acceptable Use Directive published by the University and the institutions providing the network and services in question.

6.16.7 It should be remembered that the University is being represented when correspondences being conducted using University e-mails. No insulting, offensive, detrimental, or transgressive e-mails can be sent to a user and/or group inside or outside of the University. Inappropriate content (political propaganda, racism, pornography, a material containing intellectual property etc.) cannot be sent via e-mail.

6.16.8 As prescribed by security policies, every e-mail transferred inside University systems goes through a content filtration. Some e-mails can be blocked, deleted or when deemed necessary inspected, according to the content it contains.

6.16.9 Users cannot access any kind of information, software belonging to the University or other files (including programs, subroutine library members, data, and e-mails), without obtaining permission from the related University personnel, information security official or the related party beforehand; they cannot change, copy, carry or remove the information, software and files in question.

6.16.10 Users cannot copy, distribute, view, or disclose software belonging to third parties before getting a permit from the licensor first. Users cannot install software that has not been licensed properly for use, in systems.

6.16.11 No information system belonging to the University can be used irresponsibly or in a manner that would hinder the business of others. This includes; insulting, abrasive, or harassing content and chain letters, unauthorized mass mails or forwarding or unwanted advertisement or it being made accessible; damaging a system, material or data which does not belong to the user deliberately, due to negligence or carelessness; deliberately suspending electronic communication or violating the privacy of others via other means or accessing information not belonging to the user or not intended for the user; deliberate misuse of system resources or enabling misuse of others or downloading software or data to administrative systems from unsafe sources such as free software.

6.16.12 University is in no way responsible for content which it did not personally provide to information systems. Users access the content provided by others by accepting that he/she may find them insulting, inappropriate or harmful and risk falls on the user. Information systems are presented "as they are" and "in their present state". The University holds itself exempt from all kinds of obligations regarding the content of thirds parties being true, full, and credible. User

is personally responsible for the information that he/she keeps or preserves in information systems being legal or illegal.

6.16.13 The user accepts that all attempts at any kind of action which would prevent information systems' operation or would prevent the information systems in question from being used by others; uploading content to information systems which would cause overload; actions which would pose a danger against overall security of information systems and/or would damage other users; using or trying to use software which would block or intervene in the operation of information systems are absolutely forbidden.

6.16.14 Users cannot use the internet access provided by the University for illegal transactions and activities, and in a manner which contravenes other directives, procedures, and guides/manuals of the University or which would harm the University. Users cannot act in a way that would disturb others or would infringe the individual rights of others.

6.16.15 There should not be a direct internet connection from personal laptops to the University network. Internet gateway and institutional VPN of the University has been established for this reason and users must connect the University network over the Internet by using the VPN and connect to the Internet via the gateway, from a single port. Attempts at obtaining unauthorized access to resources in the network, seizing or rerouting network connections are forbidden.

6.16.16 Every document which will be destroyed, will be destroyed according to the Storing and Destroying Personal Data Directive. Other documents that are not classified will not be left at random areas inside or outside the office and will be put in recycle bins.

6.17 All non-defined matters related to this directive are applied only with the approval of the Information Security Committee.

7. METHOD

7.1 Information Security Committee is informed in the event of unauthorized use or misuse of the University's information systems, contravening or violation of the University's directives is being detected. The Committee will govern the required process.

8. ANNEXES AND RECORDS

None.

9. REVIEW

Information Technologies Directorate has the responsibility to review and update this document. Reviews are conducted at least once a year. The document needs to be revised at times and in situations where it is deemed necessary.

10.   CHANGES/ DISTRIBUTION/ APPROVAL TABLE

Changed Pages	Date	Change	Person Who Performed the Change
-	27.01.2022	The review has been done. There is no change.	-
Distribution (Related Departments)			
Entirety of the Koç University			