Consequences of IT Service Abuse in Brief

The IT service rules of the University of Applied Sciences bind and obligate all users of IT services and systems. Including you.

The term 'IT service abuse' refers to service use in a manner that is against the IT service rules or applicable laws. All detected cases of abuse must be reported to the Head of IT Services.

In case of suspected abuse, the university of applied sciences can restrict the user's access to services for the duration of the related investigation. Depending on the severity and intentionality of the act, service abuse can lead to consequences within the university of applied sciences or be reported to the police.

Further specifications to these rules are provided below:

Consequences of IT service abuse

IT service abuse means activities that are against the IT service rules of the University of Applied Sciences or Finnish laws.

This document outlines the measures applied to the suspected party when a case of IT service abuse has been detected or there is justified reason to suspect such abuse. The measures range from restricting access rights during the investigation of a suspected abuse case to implementing actual consequences after the abuse has been confirmed.

The university of applied sciences can restrict access to its services during abuse investigation

When a breach of IT service rules has been detected or there is reason to suspect one, the University of Applied Sciences can decide to set access rights restrictions to the user in question. Access rights are restricted whenever there is justified reason to suspect that a user has abused the services and that the continued use of his/her rights would harm the investigation of the case or hinder damage control. When necessary, the user is invited to a hearing.

The decision to restrict access rights is made by the Head of IT Services or any another authorised person. The restrictions are implemented by the service's system administrator.

In urgent cases, the system administrator can independently set access restrictions for a maximum of three days, and this must be immediately reported to the security specialist in charge of restrictions.

When necessary, a user's workstation can be disconnected from the network.

The access restrictions can be removed once the investigation is completed, if the restoration of the user's rights does not pose an evident risk.

Consequences

In minor cases of abuse, the user receives a notice of improper activity.

A user found guilty of IT system abuse can be deemed liable to pay compensation for the abused resources (e.g. servers or network), direct damages and the costs of investigating the abuse.

Consequences to students

Consequences applicable to students include a temporary loss or restriction of usage authorisation, administrative actions by the University of Applied Sciences (written notice, temporary suspension), or reporting the case to the police (if the act is punishable under a law).

Consequences concerning usage authorisation are determined by the IT management. The term of restricted authorisation does not include the time spent investigating the case. Written notices are issued upon the decision of the President of the University of Applied Sciences, and suspension decisions are made by the Board of the Univeristy of Applied Sciences. If a student is suspended, his/her IT system usage authorisation is revoked for the duration of the expulsion.

The minimum period of usage authorisation restriction applied in such cases is outlined in the abuse penalty table.

Consequences to staff members

Consequences applicable to staff members of the University of Applied Sciences include labour-law actions (written notice, dismissal, termination of employment contract) or reporting the case to the police (if the act is punishable under a law).

The user's access to certain systems can be temporarily or permanently denied due to the lack of confidence caused by the abuse. Consequences concerning usage authorisation are determined by the Head of IT Services.

Consequences to other users

Consequences applicable to users with roles other than degree student or staff member include the cancellation or restriction of usage authorisation or reporting the case to the police (if the act is punishable under a law).

The user's access to certain systems can be temporarily or permanently denied due to the lack of confidence caused by the abuse. Consequences concerning usage authorisation are determined by the Head of IT Services.

Tables of penalties

The tables attached to this document (Appendix 1) outline the recommended penalties for breaches of IT service rules applicable to students of the University of Applied Sciences, staff members and other users.

The tables contain examples of typical IT system abuse cases classified by severity. In addition to the severity of the act, the level of intention is taken into account when determining the consequences. In case of users who are both students and staff members, the staff members' table shall apply.

Examples of IT service abuse

– Unauthorised handling of material subject to the Criminal Code and Copyright Act.

+ Material subject to the Criminal Code includes, for example, child porn, zoophilia, extreme violence, racist material and agitation
+ handling includes the possession and distribution of such material.
- Material subject to the Copyright act includes music, videos, comic strips, movies, games and software.
- Handing over user IDs includes
+ revealing your password to another user

+ leaving the workstation session open so that another user can continue using it under your ID.
- Compromising the confidentiality of information includes
+ disclosing information that is classified as secret or otherwise protected by law to an unauthorised person (for example, handingover server user data)
+ neglecting the information security of confidential information (passive negligence)
+ intentional breaches of confidentiality (active offense)
+ breaching the Personal Data Act.
- Negligence of personal information security includes
+ Leaving your password on sight
+ neglecting to use the University of Applied Sciences' back-up copy procedures.

Validity

These rules become effective 1 January 2014 onwards and replace all earlier versions of corresponding rules.

Further information

The instructions referred to or related to by these instructions are:

- IT Service User Rules
- Email rules
- Retrieving and Opening an Employee's Email
- Consequences of IT Service Abuse (this document)
- Tables of Penalties of IT Service Abuse
- Administrative Rules for Information Systems

Appendices

Appendix 1: Recommendations of the IT service abuse consequenses, students, staff members

Karelia, appendix 1

TABLE OF PENALTIES, students

LEVEL OF INTENT ▶	Unawareness Incompetence Negligence Accident Lack of intent	Carelessness Gross negligence Ignorance Proving a point Intent Recurrence	Criminal intent (damage, unauthorised use, espionage, confidentiality offence, abuse of public office etc.) Pursuit of gain
▲ SEVERITY OF OFFENCE			
Serious offence (an act that constitues a misdemeanour or crime under the law), such as			
* Hacking	Reporting of the offence to the police considered	Reporting of the offence to the police considered	Reporting of the offence to the police
* Unauthorised handling of material subject to the Criminal Code			
* Unauthorised distribution of material subject to the Copyright Act	Written notice possible	Temporary expulsion	Temporary expulsion
* Deliberate, unauthorised port scanning			
* Deliberate distribution of malware	Notice / Access rights	Access rights restriction 3 - 6 months	Access rights restriction 6 months >
* Denial of service attack	restriction 1 week - 3 months		
Offence (gross abuse or security risk), such as			
* Unauthorised copying of applications and games			Reporting of the offence to the police considered
* Installing of unauthorised applications			
* Unauthorised possession of hacking/administration tools		Written notice	Temporary expulsion
* Unauthorised service set-up			
* Handing over an ID	Notice / Access rights		
* Risking confidentiality of information	restriction 1 week - 2 months	Access rights restriction 1 - 3 months	Access rights restriction 3 - 6 months
Minor offence (negligence), such as			
* Neglecting personal information security			Reporting of the offence to the police considered
* Improper behaviour			
* Causing disturbance			
* Wasting IT resources			
* Neglecting the use of security software and updates	Notice / Access rights	Access rights restriction 1 week - 2 months	Access rights restriction 1 - 3 months
* Forbidden commercial or political activity	restriction 1 week - 1 month		
* Breach of physical access monitoring rules			
▲ SEVERITY OF OFFENCE			

The user's access to centrain systems can be temporarily or permanently denied due to the lack of confidence caused by abuse.

Penalty classification:

	Possible reporting of an offence to the police
	General administrative actions
	Actions according to UAS instructions or consequences determined by the Head of IT Services

Karelia, appendix 1

TABLE OF PENALTIES, staff

LEVEL OF INTENT ▶	Unawareness Incompetence Negligence Accident Lack of intent	Carelessness Gross negligence Ignorance Proving a point Intent Recurrence	Criminal intent (damage, unauthorised use, espionage, confidentiality offence, abuse of public office etc.) Pursuit of gain
▲ SEVERITY OF OFFENCE			
Serious offence (an act that constitues a misdemeanour or crime under the law), such as			
* Hacking	Reporting of the offence to the police considered	Reporting of the offence to the police	Reporting of the offence to the police
* Unauthorised handling of material subject to the Criminal Code			
* Unauthorised distribution of material subject to the Copyright	Notice/written notice possible	Written notice / dismissal / termination of employment contract	Termination of employment contract
* Deliberate, unauthorised port scanning			
* Deliberate distribution of malware			
* Denial of service attack			
Offence (gross abuse or security risk), such as			
* Unauthorised copying of applications and games			Reporting of the offence to the police
* Installing of unauthorised applications			
* Unauthorised possession of hacking/administration tools	Notice/written notice possible	Written notice / dismissal / termination of employment contract	Dismissal / termination of employment contract
* Unauthorised service set-up			
* Handing over an ID			
* Risking confidentiality of information			
Minor offence (negligence), such as			
* Neglecting personal information security			Reporting of the offence to the police considered
* Improper behaviour			
* Causing disturbance	Notice	Notice/written notice possible	Written notice / dismissal / termination of employment contract
* Wasting IT resources			
* Neglecting the use of security software and updates			
* Forbidden commercial or political activity			
* Breach of physical access monitoring rules			
▲ SEVERITY OF OFFENCE			

The user's access to centrain systems can be temporarily or permanently denied due to the lack of confidence caused by abuse.

Penalty classification:

Possible reporting of an offence to the police

General administrative actions

Karelia, appendix 1

TABLE OF PENALTIES, other users

LEVEL OF INTENT ▶	Unawareness Incompetence Negligence Accident Lack of intent	Carelessness Gross negligence Ignorance Proving a point Intent Recurrence	Criminal intent (damage, unauthorised use, espionage, confidentiality offence, abuse of public office etc.) Pursuit of gain
▲ SEVERITY OF OFFENCE			
Serious offence (an act that constitutes a misdemeanour or crime under the law), such as			
* Hacking	Reporting of the offence to the police considered	Reporting of the offence to the police	Reporting of the offence to the police
* Unauthorised handling of material subject to the Criminal Code			
* Unauthorised distribution of material subject to the Copyright Act			
* Deliberate, unauthorised port scanning			
* Deliberate distribution of malware	Notice / Access rights	Revoking access rights	Revoking access rights
* Denial of service attack	restriction 1 week - 3 months (students) / revoking access rights		
Offence (gross abuse or security risk), such as			
* Unauthorised copying of applications and games			Reporting of the offence to the police
* Installing of unauthorised applications			
* Unauthorised possession of hacking/administration tools			
* Unauthorised service set-up			
* Handing over an ID	Notice / Access rights	Revoking access rights	Revoking access rights
* Risking confidentiality of information	restriction 1 week - 2 months (students)		
Minor offence (negligence), such as			
* Neglecting personal information security			Reporting of the offence to the police considered
* Improper behaviour			
* Causing disturbance			
* Wasting IT resources			
* Neglecting the use of security software and updates			
* Forbidden commercial or political activity	Notice / Access rights	Notice / Access rights	Revoking access rights
* Breach of physical access monitoring rules	restriction 1 week - 1 month (students)	restriction 1 week - 2 months (students) / revoking access rights	
▲ SEVERITY OF OFFENCE			

The user's access to centrain systems are denied due to the lack of confidence caused by abuse.

Penalty classification:

Possible reporting of an offence to the police

Actions according to UAS instructions or consequences determined by the Head of IT Services