NUTZUNGSORDNUNG INFORMATIONSTECHNOLOGIE FÜR KOOPERARTIONSPARTNER

REGULATIONS FOR THE USE OF INFORMATION TECHNOLOGY FOR COOPERATION PARTNER

NUTZUNGSORDNUNG INFORMATIONSTECHNOLOGIE

Version: V 2 (Auszüge aus „Nutzungsordnung Informationstechnologie“ V2 vom 6.2.2018
Date: 22. November 2018

INHALT

1. ZIELGRUPPE & GELTUNGSBEREICH

Diese Nutzungsordnung regelt die Nutzung aller zentralen und dezentralen Informationsverarbeitungssysteme und -infrastrukturen im DKFZ (IT-Systeme) und ist verbindlich für ***Kooperationspartner,*** d.h. Mitglieder anderer Forschungseinrichtungen bzw. sonstige natürliche Personen, die eine Nutzungserlaubnis (UserID) auf Grundlage besonderer Kooperations- oder Dienstleistungsvereinbarungen erhalten haben. Diese Personen dürfen die IT-Systeme nur unter Verwendung einer personalisierten UserID und nur im Rahmen ihrer Aufgabenerfüllung unter Beachtung der IT-Sicherheitsvorschriften nutzen.

Mit der zugeordneten User-ID kann ein Kooperationspartner unter Verwendung zugriffssicherer Methoden über das Internet auf die Kooperationsplattformen des DKFZ zugreifen. Zusätzlich kann sich der Kooperationspartner in den Räumlichkeiten des DKFZ mit seiner UserID an einem DKFZ-Arbeitsplatz anmelden und erhält Zugang zum Internet sowie zu Druckern, die an diesem Arbeitsplatz verfügbar sind. Wenn der Kooperationspartner sein eigenes Notebook verwenden möchte, erhält er über das vorhandene drahtlose Netzwerk Zugang zum Internet.

2. EINVERSTÄNDNISERKLÄRUNG DER BENUTZER

Durch die Übernahme der Nutzungserlaubnis, in der Regel einer UserID (siehe Kapitel 6), erklärt sich die Benutzerin bzw. der Benutzer mit Folgendem einverstanden:

1. Die personenbezogenen Anmeldedaten dürfen für die UserID-Pflege verarbeitet werden.
2. Die Nutzung persönlich zugeordneter, dienstlicher Daten des Benutzers ist der Leitung der Organisationseinheit in Absprache mit der in Kapitel 4 genannten IT-Sicherheitskommission gestattet, sofern der Benutzer selbst nicht vorher informiert werden konnte.
3. Die Nutzungserlaubnis ist auf die gültige Kooperations- oder Dienstleistungsvereinbarungen beschränkt und ist grundsätzlich zeitlich befristet. Sie erlischt mit Wegfall des Zulassungsgrundes, kann aber auf Antrag verlängert werden.
4. Es werden UserID- und Netzwerkadressen-bezogene Ereignisprotokolle angefertigt, in denen IT-sicherheitsrelevante Ereignisse an einem besonders gesicherten Ort aufgezeichnet werden. Diese Protokolle werden zwei Jahre aufbewahrt und danach automatisch gelöscht. Sie werden ausschließlich für interne IT-Sicherheitsüberprüfungen von eigens dafür geschultem Personal in der ITCF bzw. von beauftragten Sicherheitsfirmen verwendet. Bei der Verarbeitung von personenbezogenen Daten werden gemäß gesetzlicher Auflagen die Verarbeitungsschritte mitprotokolliert. Diese Protokolle werden ebenfalls besonders gesichert und verschlüsselt für fünf Jahre aufbewahrt und danach gelöscht. Die Sichtung dieser Protokolle darf nur auf schriftlichen Antrag und in Absprache mit der in Kapitel 3 genannten IT-Sicherheitskommission geschehen.

3. VERFAHRENSWEISE BEI VERSTOß GEGEN REGELUNGEN

Bei Verdacht auf Verstoß gegen Regelungen in dieser Nutzungsordnung, der weiterführenden Regelungen bzw. der geltenden Dienstvereinbarungen wird auf formlosen Antrag (per E-Mail, Telefon) eine IT-Sicherheitskommission tätig, die den Sachverhalt klärt. Diese IT-Sicherheitskommission besteht aus jeweils einem Mitglied der Personalabteilung, des Personalrates, der ITCF sowie dem/r Datenschutzbeauftragten und dem/der IT-Sicherheitsbeauftragten und berichtet bei bestätigtem Verdacht an den Vorstand. Der Dienststelle obliegt es, dann gegebenenfalls weitere individualrechtliche Schritte einzuleiten. Der/Die IT-Sicherheitsbeauftragte berichtet dem/der Compliance-Beauftragte/n.

4. NUTZUNGSERLAUBNIS

Die Zuteilung einer Nutzungserlaubnis erfolgt durch die ITCF oder im Ausnahmefall und für spezielle IT-Systeme durch Fachabteilungen, die von der ITCF autorisiert wurden und die die zentrale UserID-Verwaltung nicht nutzen können.

Die Nutzungserlaubnis für IT-Systeme ist in der Regel personenbezogen und besteht aus UserID und Passwort.

Jeder Benutzer ist verantwortlich für die Geheimhaltung und Sicherheit seiner persönlichen Nutzungserlaubnis bzw. die Einhaltung von Vorgaben zu Verfahrensweisen von nicht-persönlich zugeordneten Nutzungserlaubnissen.

Passwörter sind entsprechend den von der IT Core Facility festgelegten und mit den zuständigen Gremien im Haus vereinbarten Regeln zu setzen.

Die Weitergabe von UserIDs und Passwörtern an Dritte ist nicht gestattet. Der Benutzer ist für alle Handlungen, die unter seiner Benutzerkennung durchgeführt werden, verantwortlich - auch wenn diese Handlungen von Dritten ausgeführt werden, denen er die Zugangsdaten weiter gegeben hat.

5. VERHALTEN BEI IT-SICHERHEITSVORFÄLLEN

Einen meldepflichtigen Sicherheitsvorfall stellt jedes Ereignis dar, welches Einfluss insbesondere auf Vertraulichkeit und Integrität von Daten bzw. auf die nicht ordnungsgemäße Nutzung der IT haben kann.

Beispiele hierfür sind:

1. Daten in einem IT-System sind verfälscht
2. Ungewöhnliches Verhalten von IT-Systemen wie z.B. Veränderung der Startseite des Webbrowsers

3. Verdacht des Missbrauchs der eigenen oder einer anderen UserID

Sofern ein Sicherheitsvorfall festgestellt oder Kenntnis hierüber erlangt wurde, muss der Verantwortliche der entsprechenden Kooperation umgehend informiert werden.

6. ALLGEMEINE NUTZUNGSREGELUNGEN

Die IT-Systeme dienen grundsätzlich der Erfüllung der dienstlichen Aufgaben und dürfen nur im Rahmen ihrer Zweckbestimmung wirtschaftlich und verantwortungsvoll genutzt werden.

Die Weitergabe von geheimhaltungsbedürftigen Informationen, die dem Benutzer im Zusammenhang mit der Tätigkeit am DKFZ bekannt werden, ist entsprechend der gesetzlichen, tariflichen und arbeitsvertraglichen Regelungen nicht gestattet. Dies gilt insbesondere für personenbezogene Daten jeglicher Art sowie für patentfähige Erkenntnisse und Tatsachen.

6.1. VERLASSEN DES ARBEITSPLATZES

IT-Systeme sind bei Verlassen des Arbeitsplatzes so zu sichern, dass kein Unbefugter Zugriff auf Daten und Informationen erhalten bzw. durch Herunterfahren des IT-Systems noch nicht gespeicherte Daten löschen kann. Dies gilt insbesondere für alle Bereiche, in denen personenbezogene oder vertrauliche Daten verarbeitet werden bzw. für offen zugängliche Arbeitsplätze.

Beim Verlassen des Arbeitsplatzes für einen geplanten längeren Zeitraum, wie z.B. für eine Besprechung, sind sämtliche Daten zu speichern und offene Programme nach Möglichkeit zu schließen. Nach Arbeitsende ist das Endgerät herunterzufahren und abzuschalten.

DEUTSCHES KREBSFORSCHUNGSZENTRUM

REGULATIONS FOR THE USE OF DKFZ INFORMATION TECHNOLOGY THROUGH EXTERNAL PARTNERS

Version: V 2 (extracts of DKFZ's "Regulations for the Use of Information Technology" V2 6 Feb 2018)
Date: 22 Nov 2018

CONTENTS

1. TARGET AUDIENCE & SCOPE OF APPLICATION

These Terms of Use govern the use of all centralised and decentralised information processing systems and infrastructures at the DKFZ (IT systems) and apply to ***cooperation partners***, i.e. members of other research institutes or other natural persons, who have been granted a usage license (userID) on the basis of a special cooperation or service agreement. Such persons may only use the IT systems with a personalised user ID, and may only do so within the context of completing the work that has been allocated to them, and only under observance of the IT security regulations.

With his or her user ID, a cooperation partner can access the cooperation platforms at DKFZ using secure methods via the Internet. In addition, the cooperation partner can log in on the premises of the DKFZ using his or her user ID on a DKFZ terminal and receives access to the Internet and access to the printers available on that terminal. If the cooperation partner wants to use his or her own notebook, he or she receives access to the Internet via the existing wireless network.

2. USER'S DECLARATION OF AGREEMENT

By accepting the usage license, which is usually a user ID (see section 4), the user declares that they agree with the following:

1. The personal login details can only be processed for the purposes of user ID maintenance.
2. The user's business data that can be traced back to them personally may be used by the management of the organisational unit in consultation with the IT Security Committee mentioned in section 3 in the event that it was not possible to inform the user themselves in advance.
3. The usage license is limited to the context of the applicable cooperation agreement or service agreement and is always time-limited. It expires when the reason for the permission no longer applies, but can be extended on request if required.
4. User ID and network address-related event logs will be created, in which events that are relevant to IT security will be recorded at a specially secured location. These logs are retained for two years, and after this period they are automatically deleted. They are used only for internal IT security checks conducted by specially trained ITCF staff, or by contracted security companies. During the processing of personal data, the processing steps are recorded at the same time in accordance with legal obligations. These logs are also given special security protection and are stored in encrypted form for five years. After this period they are deleted. Inspection of these logs is by written request only and may occur only in consultation with the IT Security Committee mentioned in section 3.

3. PROCEDURE IN THE EVENT OF VIOLATION OF REGULATIONS

In the event of a suspected violation of these Terms of Use or the applicable service agreements, the IT Security Committee will act to clarify the facts of the case upon informal request (e.g. by e-mail or telephone). This IT Security Committee consists of one member from the HR Department, one member from the Staff Council, one member from the ITCF, the Data Protection Officer, and the IT Security Officer, and it reports to the Board of Directors in the event that a suspicion is confirmed. Thereafter, the IT Security Committee is responsible for taking further legal steps against individuals if necessary. The IT Security Officer reports to the Compliance Officer.

4. USAGE PERMISSIONS

Usage permissions are issued by the ITCF, or in exceptional cases and for special IT systems by specialist departments that have been authorised to do so by the ITCF because they cannot use the centralised user ID management system.

Usage permissions for IT systems are usually personalised and are composed of a user ID and password.

Every user is responsible for maintaining the confidentiality and security of their own usage permissions and for complying with regulations regarding procedures for usage permissions that have not been assigned to specific individuals.

Passwords must be set up in accordance with the rules that have been defined by ITCF and agreed upon with the competent in-house bodies.

The transfer of user IDs and passwords to third parties is not permitted. The user is responsible for all actions carried out under his user ID, even if these actions are carried out by third parties whom he has granted access to.

5. PROCEDURE IN THE CASE OF AN IT SECURITY BREACH

An IT security breach that must be reported is defined as any incident that could affect the confidentiality and integrity of data or that may be related to improper use of IT.

Examples include:

1. Data within the IT system that has been falsified
2. Unusual behaviour of IT systems
3. Suspected misuse of a person's own user ID, or of that of another person

The person responsible for a cooperation must be informed immediately about any security breach that is established or discovered.

6. GENERAL USAGE REGULATIONS

The purpose of the IT systems is to allow business tasks to be completed. They may only be used within the context of their intended purpose and must be used economically and responsibly.

The disclosure of confidential information that becomes known to the user in connection with their activities within the DKFZ is not permitted, as set forth in legal, collective bargaining, and employment contract regulations. This applies in particular to personal data of any kind, and to knowledge and facts that may be patentable.

6.1. LEAVING THE WORKPLACE

When leaving the workplace, IT systems must be secured in such a way that no unauthorised persons can gain access to data and information, or delete data that has not yet been saved by shutting down the IT system. This applies in particular to all areas in which personal or confidential data is processed, and to publicly accessible workplaces.

When leaving the workplace for a planned, extended period, for example when leaving for a meeting, all data must be saved and any open programs should be closed as far as possible. At the end of the working day, the terminal must be shut down and switched off.