Informations-sicherheitsleitlinie

der

Hochschule für Musik und Darstellende Kunst

Frankfurt am Main

Amtliche Bekanntmachungen
der Hochschule für Musik und Darstellende Kunst
Frankfurt am Main

Veröffentlichungsnummer: 108/2022 In Kraft getreten am: 16.02.2022

Präambel

Die Hochschule für Musik und Darstellende Kunst Frankfurt am Main entwickelt sich im Bereich Informationssicherheit zu einer modernen Kunsthochschule, in deren Lehre und Verwaltung der Umgang mit Informationen eine wesentliche Rolle spielt. Prozesse zur Aufgabenerfüllung in den verschiedenen Arbeitsbereichen der Hochschule werden wesentlich durch Informationstechnologie (IT) unterstützt. Die zunehmende Zahl IT-basierter Arbeitsprozesse lässt die Verfügbarkeit einer sicheren und zuverlässigen IT-Infrastruktur zu einem entscheidenden Faktor werden. Gemeinsam genutzte Systeme und Infrastrukturen bilden den Kern vieler Prozesse. Damit wird ein Raum gemeinsamer Sicherheit aber auch gemeinsamer Sicherheitsbedrohungen geschaffen.

Vor dem Hintergrund steigender Cyber-Kriminalität und zunehmender Angriffe auf die IT Systeme nicht nur in der privaten Wirtschaft, sondern auch in öffentlichen Einrichtungen, kommt der Informationssicherheit in der HfMDK zentrale Bedeutung zu.

Der **hohen Bedeutung der Informationssicherheit auch im öffentlichen Dienst** hat die Landesregierung Hessens mit ihrer Informationssicherheitsleitlinie Rechnung getragen. In dieser Leitlinie werden alle Bereiche des öffentlichen Dienstes verpflichtet, Strukturen aufzubauen, um die Informationssicherheit zu erhöhen. Nicht nur die **zentralen** IT-Systeme müssen gegen Angriffe und Bedrohungen geschützt werden, sondern insbesondere auch die **dezentralen** IT-Arbeitsplätze (mobile Endgeräte wie Smartphone, Tablet oder Notebook). Neben technischen Vorkehrungen steht der Faktor Mensch im Fokus, dem besondere Aufmerksamkeit gewidmet werden muss.

Die Hochschule ist aufgefordert, die vom Land Hessen vorgegebene, verbindliche Informationssicherheitsleitlinie (2021) für die Hessische Landesverwaltung umzusetzen.

Die **„Informationssicherheitsleitlinie der HfMDK“** leitet aus den Vorgaben räumliche, personelle, organisatorische und technische Sicherheitsanforderungen zum Schutz von Informationen und Daten ab und appelliert an das Verhalten und Sicherheitsbewusstsein **aller Hochschulmitglieder und –angehörigen (inkl. Lehrbeauftragten).** Es ist wichtig, dass der **Schutz der IT als gemeinsame Herausforderung akzeptiert und gelebt** wird. Ein vertrauensvolles und konstruktives Arbeitsklima, in dem Eigenverantwortung einen hohen Stellenwert besitzt, bildet die beste Grundlage für einen weitestgehend reibungslosen, sicheren und effektiven Gebrauch der Informationstechnik. Die Leitlinie wird in regelmäßigen Abständen überarbeitet.

Basierend auf der *Benutzungsordnung für die Informationsverarbeitungssysteme der Hochschule für Musik und Darstellende Kunst Frankfurt am Main v. 24.05.2011* stellt diese Leitlinie eine Ausweitung und Detaillierung der Regeln für Betrieb und Nutzung der Rechner und Netze in Bezug auf die Informationssicherheit dar.

Begriffsbestimmungen und Geltungsbereich

Informationstechnologie (IT) umfasst die Gesamtheit der genutzten Systeme und Kommunikationstechnik und die auf dieser Basis realisierten fachlichen IT-Anwendungen.

IT-Verfahren:
Eine oder mehrere IT-Anwendungen und deren begleitende Geschäftsprozesse zur Realisierung einer fachlichen Aufgabe.

Informationssicherheit beinhaltet den Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von Daten unter besonderer Berücksichtigung der datenschutzrechtlichen und sonstigen gesetzlichen Vorgaben. Da Informationen heute überwiegend mittels IT erstellt, gespeichert, transportiert und weiterverarbeitet werden, führt das zum Begriff der „IT-Sicherheit". *Integrität* ist gewährleistet, wenn schützenswerte Daten unversehrt und vollständig bleiben und nicht verfälscht werden können. *Vertraulichkeit* ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis nehmen können und sie für unberechtigte Dritte nicht zugänglich sind. *Verfügbarkeit* bezieht sich auf Daten und Verfahren und bedeutet, dass sie, wenn sie benötigt werden, auf Anfrage zeitgerecht zur Verfügung stehen.

Die **Informationssicherheitsleitlinie ist verbindlich für alle Hochschulmitglieder und –angehörigen (inkl. Lehrbeauftragte) der HfMDK**, die an Prozessen der Informationsverarbeitung beteiligt sind. Diese Prozesse beinhalten sowohl die Erstellung und Speicherung als auch die Weiterverarbeitung von Informationen.

Weiterhin ist die **Informationssicherheitsleitlinie auch verbindlich für Personen, denen durch Vereinbarungen** die Benutzung von IT-Systemen (Clients, Server, Netzkopplungselementen, Mobile Devices) sowie eingesetzten Netzen und Kommunikationseinrichtungen inkl. externen Schnittstellen (z.B. zu behördlichen oder landesweiten Systemen) der Hochschule für Musik und Darstellende Kunst Frankfurt am Main möglich ist und die Zugriff auf Daten der HfMDK haben.

Verstöße gegen die Verhaltensregeln dieser Leitlinie können dienst- oder arbeitsrechtliche Konsequenzen nach sich ziehen.

Hinweis: Die Regelungen dieser Leitlinie in Bezug auf zentrale Datenspeicherung in der HfMDK-Umgebung und Verwendung vom Rechenzentrum freigegebener Hard- und Software sind für den Bereich der Lehre vor dem Hintergrund der bestehenden

technischen Gegebenheiten im laufenden Hochschulpakt bis 2025 nicht vollständig umsetzbar.

1. Grundsätze

In Abwägung des Schutzbedarfs der Daten und Informationen, der Risiken sowie des Aufwands an Personal- und Finanzmitteln für Informationssicherheit soll für die bereits eingesetzte und für zukünftig geplante IT in der HfMDK ein angemessenes IT-Sicherheitsniveau aufrechterhalten und ausgebaut werden. Dabei ist zwischen Daten mit einfachem Schutzbedarf und sensiblen Daten mit erhöhtem Schutzbedarf zu unterscheiden.
Die Hochschule richtet sich in allen Regelungen der Informationssicherheit nach den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Informationssicherheitsleitlinie für die Hessische Landesverwaltung.
Oberstes Ziel der IT-Sicherheitsvorkehrungen ist es, die IT-Grundwerte Integrität, Vertraulichkeit und Verfügbarkeit im jeweils erforderlichen Maße zu schützen und somit die Arbeits- und Handlungsfähigkeit der Hochschule aufrechtzuerhalten.

2. Sicherheitsaspekte

Um möglichen Risiken und Schäden für die Hochschule vorzubeugen, ist es wichtig, die folgenden räumlichen, personellen, organisatorischen und technischen Sicherheitsmaßnahmen zu beachten und einzuhalten.

2.1 Räumliche Sicherheitsmaßnahmen

2.1.1 Büroräume

Vertrauliche Daten, Informationen und Unterlagen sind von den Mitarbeiterinnen und Mitarbeitern so zu schützen, dass Dritte keine Einsicht und/oder Zugriff nehmen können. Diese Daten, Unterlagen etc. dürfen nur datenschutzkonform entsorgt werden.

Der Arbeitsplatz ist mit Beendigung der Arbeitszeit so zu hinterlassen, dass unbefugten Personen kein Zugriff auf Informationen und IT-Systeme ermöglicht wird. Büroräume sind beim Verlassen abzuschließen. Bei längerer Abwesenheit und nach Dienstschluss sind die Fenster zu schließen. Schutzbedürftige Daten sind nach Möglichkeit verschlossen aufzubewahren. Unbefugte Personen dürfen nicht allein im Büroraum zurückgelassen werden. Der PC ist zu sperren.

2.1.2 Mobiles Arbeiten und Telearbeit

Mobiles Arbeiten mit Laptop, Tablet o.ä. ist auch an der HfMDK möglich. Das tägliche Arbeiten mit mobilen Endgeräten birgt besondere Sicherheitsrisiken und stellt ein leichtes Einfallstor für Angriffe von außen dar. Der Schutz durch Software,

Sicherheitsupdates sowie sichere Verbindungen alleine reicht nicht aus. Jede*r Mitarbeiter*in ist aufgefordert, das Bewusstsein für mögliche Gefahren zu schärfen, da jede einzelne Person beim mobilen Arbeiten oder bei der Telearbeit eine stärkere Verantwortung für die IT-Sicherheit erhält. Die Verbindung zum Aktenplan wird von der HfMDK über einen sicheren Virtual Private Network Client (VPN) hergestellt. Dabei wird ausschließlich auf Servern der Hochschule gearbeitet, was sicherstellt, dass keine Daten die Hochschule verlassen.

Folgende Maßnahmen sollen das mobile Arbeiten oder die Telearbeit absichern:

- Einrichtung eines klar definierten Arbeitsplatzes
- Der Bildschirm ist bei Verlassen des Arbeitsplatzes zu sperren
- Zugangsdaten sind geheim zu halten
- Informationen und Arbeitsergebnisse immer in der Serverumgebung und nicht lokal auf dem Laptop speichern, wenn die technischen Möglichkeiten dazu gegeben sind
- Dokumente sind an einem sicheren Ort aufzubewahren
- Keine Entsorgung von Dokumenten über den privaten Hausmüll (Ausdrucke sind zu schreddern oder in der Hochschule in den vorhandenen Containern für Datenvernichtung zu entsorgen)
- Daten und Informationen gegenüber Dritten einschließlich Familienangehörigen sind so zu schützen, dass Dritte diese nicht einsehen und nicht auf diese zugreifen können.
- Das Mithören dienstlicher Telefonate ist auszuschließen.
- Die Verwendung privater Endgeräte ist auf Wunsch der Hochschulangehörigen hin möglich. Der Einsatz von privaten Endgeräten erfolgt auf Kosten und Risiko der Beschäftigten.

2.1.3 Besprechungs-, Veranstaltungs- und Schulungsräume

Die Räume sind nach ihrer Nutzung abzuschließen und alle Arbeitsmaterialien zu entfernen. Geräte, die darin öffentlich zugänglich sind, sind mit Kensington Schlössern an den Möbeln gesichert. Für Geräte, die aus verschlossenen Schränken zur Benutzung im Unterricht verwendet werden, ist die Ent- und Rücknahme sicherheitskonform geregelt.

2.1.4 Archive und Funktionsräume

Unbefugte dürfen keinen Zutritt zu Archiv- und Funktionsräumen bekommen. Türen und Fenster sind verschlossen zu halten. Ausdrucke und Kopien sollen bei zentral stehenden Druckern und Kopierern nicht unbeaufsichtigt liegen gelassen werden. Die technischen Möglichkeiten des „sicheren Druckens“ mittels Abrufcode sind zu nutzen.

2.1.5 Rechenzentrum / Server- und Maschinenraum

Das Rechenzentrum ist ein besonderer Sicherheitsbereich, für den gesonderte Regelungen Anwendung finden. Der Zutritt ist nur autorisierten Personen gestattet. Für den genannten Bereich ist ein Schloss verbaut, das (aus Sicherheitsgründen)

nicht in die Schlüsselhierarchie der Hochschule integriert ist. Schlüssel haben außer den Technikern des Rechenzentrums der Hausdienst (Safe) sowie die Feuerwehr. Zutrittsberechtigungen sind auf das für den Betrieb der Hochschule erforderliche Maß beschränkt. Muss Fremdpersonal den Raum betreten, ist ein/e Mitarbeiter*in des Rechenzentrums mit vor Ort. Es werden in einer Liste in der Vor- und Zuname, Arbeitsbereich und Beginn und Ende des Betretens verzeichnet. Das Rechenzentrum besitzt kein Fenster das geöffnet werden kann. Die Zugangstür entspricht hohen Einbruchsrichtlinien. Der Raum für die Administration hat durch mechanische Sicherheitsstangen geschützte Fenster. Außerdem sind alle Fenster abgeschlossen. Die Reinigung der Räume wird durch das Rechenzentrum vorgenommen, es wird kein externes Reinigungspersonal eingesetzt.

2.2 Personelle Sicherungsmaßnahmen

Alle Hochschulmitglieder und –angehörigen (inkl. Lehrbeauftragte) gewährleisten die Informationssicherheit durch ihr verantwortungsbewusstes Handeln.

2.2.1 Vertretungsregelung

Für vorhersehbare (Urlaub, Dienstreisen) und unvorhersehbare Fälle (Krankheit, Unfall) des Personals, sind im Vorfeld Vertretungsregelungen festzulegen und einzurichten, um die Fortführung der Aufgabenwahrnehmung sicherzustellen. Bei vorhersehbarer Abwesenheit ist der Abwesenheitsassistent einzurichten.

2.2.2 Einweisung und Information der Hochschulmitglieder und –angehörigen (inkl. Lehrbeauftragten)

Die Informationssicherheitsleitlinie wird allen neuen Mitarbeiterinnen und Mitarbeitern ausgehändigt. Der Erhalt ist zu quittieren und wird der Personalakte beigefügt. Sie werden nach Überarbeitung der Leitlinie über Neuerungen/ Änderungen mit Bezug auf IT-Prozesse per E-Mail informiert, so dass die Anforderungen zur Aufrechterhaltung der IT-Sicherheit aktuell bekannt sind und beachtet werden können.
Das Rechenzentrum informiert im „Akut-Fall“ (Phishing, Spam-Risiken etc.) alle Beschäftigten direkt per E-Mail.

Im Rahmen des Weiterbildungsangebots der HfMDK sollen für die Beschäftigten Online-Schulungsangebote zur Informations-sicherheit bereitgestellt werden. Ziel dieser Unterweisungen wird es sein, die Nutzer*innen der Informationstechnik darin zu sensibilisieren, spezifische Gefahren zu erkennen und angemessen reagieren zu können.

Zur Sensibilisierung der Studierenden und externen Lehrenden wird die Informationssicherheitsleitlinie auf der HfMDK-Website hinterlegt und auf deren Bedeutung und Notwendigkeit der Einhaltung hingewiesen.

2.3. Organisatorische Sicherheitsmaßnahmen

Organisatorische Rahmenbedingungen der Informationssicherheit sind aufrecht zu erhalten, kontinuierlich weiterzuentwickeln und zu verbessern.

2.3.1 Aufbewahrung dienstlicher Unterlagen

Dienstliche Unterlagen dürfen nur autorisierten Personen zugänglich sein. Dies gilt sowohl für die Räume in der Hochschule als auch am mobilen Arbeitsplatz. Außerhalb der Nutzungszeit müssen sie so aufbewahrt werden, dass kein Unbefugter darauf zugreifen kann. (s. 2.1.1 und 2.1.2

2.3.2 Zutrittsvergabe und -kontrolle

Die Vergabe und Dokumentation der Zutrittsrechte (Ausgabe von Schlüsseln und Transpondern) erfolgt durch die Abt. Bau- und Gebäudemanagement. Die Ausgabe erfolgt gegen Quittung und ist zu dokumentieren. Vorhandene Reserveschlüssel oder General-Transponder sind gegen unbefugten Zugriff geschützt aufzubewahren. Die Weitergabe von Zutrittsberechtigungen ist untersagt. Bei Verlust oder Beschädigung eines Zutrittsmittels ist unmittelbar die Abt. Bau- und Gebäudemanagement zu informieren.

2.3.3 Einrichtung, Deaktivierung und Löschung von Zutrittsrechten

Im Falle des Neueintritts, Wechsels oder Austritts von Mitarbeiter*innen informiert die Abteilung Personalservice & Organisation die Abteilungen Bau-und Gebäude-management und das Rechenzentrum mindestens zwei Wochen im Voraus. Die nicht mehr benötigten Zutrittsmittel ausscheidender oder wechselnder Mitarbeiter*innen sind gegen Unterschrift an die Abteilung Personalservice & Organisation zurückzugeben. Die Rückgabe ist zu dokumentieren und wird zur Personalakte genommen.

2.3.4 Benutzerkennungen

Alle IT-Systeme werden durch Kennungen und Passwörter so eingerichtet, dass nur berechtigte Nutzer*innen mit ihnen arbeiten können. Die Arbeit unter anderer Kennung sowie die Weitergabe von Kennungen und Passwörtern ist untersagt.

2.3.5 Zugriffsrechte

Ein/e Nutzer*in darf nur mit den Zugriffsrechten ausgestattet werden, die für die Erledigung ihrer/seiner dienstlichen Aufgaben erforderlich sind. Die Vergabe, Änderung oder Löschung von Zugriffsrechten sowie deren Dokumentation erfolgt durch das Rechenzentrum. In Fachprogrammen erfolgt die Vergabe, Änderung oder Löschung durch die Fachverantwortlichen der jeweiligen Abteilung. Ihnen obliegt deren Dokumentation.

2.3.6 Besucher und externes Reinigungspersonal

In besonders schutzbedürftigen Räumen (Rechenzentrum, Personalabteilung) dürfen sich Besucher*innen und externes Reinigungspersonal nur in Begleitung von Mitarbeitern*innen aufhalten.

2.4 Technische Sicherheitsmaßnahmen

Um einen ausreichenden Schutz der Prozesse mit IT-Beteiligung zu gewährleisten, sind folgende technische Sicherheitsmaßnahmen zu beachten.

2.4.1 Sicheres Login

Jede*r Nutzer*in erhält eine eigene Kennung und ein eigenes Initial-Passwort. Die Anzahl der Anmeldeversuche wird auf 3 beschränkt. Nach dreimaliger nicht erfolgreicher Anmeldung wird der Account gesperrt.

Folgende Empfehlungen sollten bei der persönlichen Passwortvergabe beachtet werden:

- Keine gleichen Passwörter für verschiedene Programme
- Initial- oder voreingestellte Passwörter bei der erstmaligen Systemnutzung ändern
- Das Passwort sollte nicht aufgeschrieben werden
- Das Passwort darf nur dem Anwender bekannt sein
- Das Passwort darf nur eingegeben werden, wenn der Anwender unbeobachtet ist
- Keine Wiederholung von Zeichen im Passwort (xxxxyyyy)
- Keine Verwendung von Vor- oder Familiennamen und Geburtstagen
- Länge mindestens 8 Zeichen (aus Klein-, Großbuchstaben, Zahlen, Sonderzeichen)
- Benutzername darf nicht im Passwort enthalten sein

2.4.2 Bildschirmsperre

Beim Verlassen des Büros ist die Bildschirmsperre zu aktivieren. Bei fehlender manueller Aktivierung hat die Bildschirmsperre automatisch zu erfolgen.

2.4.3 Abmelden des Benutzers zum Dienstende

Die Mitarbeiter*innen sind dazu verpflichtet, sich zum Dienstschluss von den genutzten IT-Anwendungen abzumelden.

2.4.4 Datensicherung

Grundsätzlich sollten Daten auf zentralen Servern gespeichert werden. Regelmäßige Datensicherungen werden turnusmäßig durch das Rechenzentrum auf den zentralen Servern vorgenommen. Mitarbeiter*innen mit Remote-Zugriff auf die Hochschulsysteme sind verpflichtet, die Daten in den HfMDK Strukturen zu sichern.

2.4.5 Virenschutz

Aktuelle Virenscanner auf den zentralen Serversystemen und den mobilen Endgeräten sollen das Eindringen schädlicher Programme erkennen und verhindern. Auf allen Rechnern ist daher durch das Rechenzentrum ein aktueller Virenscanner eingerichtet, der automatisch alle eingehenden Daten und alle Dateien überprüft. Regelmäßig (automatisiert) sind die Virenerkennungsmuster zu aktualisieren.

2.4.6 Nutzung von Hard- und Software

Fehlerhafte oder manipulierte Hard- oder Software gefährden die Sicherheit des Datenbestandes und der Programme der Hochschule.

Deshalb sind folgende Anforderungen zu beachten:

- Es darf nur vom Rechenzentrum freigegebene Hard- und Software verwendet werden.
- Im Rahmen der Einführung neuer Software müssen die Mitarbeiter*innen ausreichend geschult werden.
- Änderungen der Einstellungen (Installation, Deinstallation, Änderungen der Konfiguration etc.) auf den hochschuleigenen Geräten sind ausschließlich dem Rechenzentrum vorbehalten.
- Die eigenmächtige Installation von Hard- und Software auf den fest installierten dienstlichen Geräten ist grundsätzlich untersagt.
- Die in den Arbeitsräumen eingesetzte Hardware darf nicht eigenmächtig in andere Räume umgesetzt werden.
- Nicht vom Rechenzentrum ausgegebene Geräte können über das WLAN in der Hochschule lokal arbeiten. Vom Nutzer ist sicherzustellen, dass die Geräte in Bezug auf ihren Virenschutz auf dem neusten Stand sind.
- Die Nutzung der vom Arbeitgeber zur Verfügung gestellten Arbeitsmittel sowie E-Mail-Adressen zu privaten Zwecken ist untersagt.
- Keine Freigabe für die Weiterleitung von E-Mails auf private Accounts bzw. Installation des Clients auf private Endgeräte.
- Datenspeicherung von dienstlichen Geräten nur auf dem HfMDK Fileserver (Aktenplan), HessenDrive oder über andere von der Hochschule freigegebene Systeme.

2.4.7 Zeitnahes Einspielen sicherheitsrelevanter Updates

Aufforderungen zu Updates aus vertrauenswürdigen Quellen werden vom Rechenzentrum nach Dringlichkeit für die zentrale Infrastruktur als auch für die verwendeten mobilen Endgeräte eingespielt. Sie sind vor der Installation mit Hilfe aktueller Virenschutzprogramme zu testen.

2.4.8 Warnhinweise des IT-Sicherheits-Ressorts des HMWK

Die Warnhinweise sind im Hinblick auf Relevanz für die Hochschule umgehend zu prüfen und -falls für die HfMDK relevant- die angegebenen Empfehlungen nach vorgegebener Dringlichkeit umzusetzen.

3 Umgang mit Sicherheitsvorfällen

3.1.1 Wann liegt ein Sicherheitsvorfall vor?

Als Sicherheitsvorfall gilt ein Ereignis, das die Verfügbarkeit, Vertraulichkeit oder Integrität von Informationen, Prozessen, IT-Systemen oder IT-Anwendungen in einer Form beeinträchtigt, die schädigend für die Hochschule ist (z.B. Virenbefall von PCs oder Laptops, Verlust oder Diebstahl von Hardware o.ä.).

3.1.2 Verhalten bei Sicherheitsvorfällen

Das Rechenzentrum und die/der Informationssicherheitsbeauftragte sind umgehend zu informieren, wenn ein IT-Sicherheitsvorfall bemerkt wird. Im Umgang mit Sicherheitsvorfällen ist Kooperationsbereitschaft und Ehrlichkeit aller Mitarbeiterinnen und Mitarbeiter besonders wichtig, um umgehend die erforderlichen Schritte einleiten zu können.

3.1.4 Dokumentation von Sicherheitsvorfällen

Das Rechenzentrum und die/der Informationssicherheitsbeauftragte sind zur Dokumentation aufgetretener bedeutsamer Sicherheitsvorfälle in der Hochschule verpflichtet. Diese Dokumentationen sind streng vertraulich zu behandeln.

3.1.3 Benachrichtigung externer Stellen

Die verantwortliche Stelle für IT Sicherheit im Ministerium muss umgehend über einen bedeutsamen Sicherheitsvorfall in Kenntnis gesetzt werden, um in Abstimmung mit der Hochschule entsprechende Gegenmaßnahmen ergreifen zu können. Die Meldung obliegt der Hochschulleitung oder einer/einem von ihr Beauftragten.

4 Kontinuierlicher Verbesserungsprozess der Sicherheitsmaßnahmen

Die dauerhafte Wirksamkeit eingerichteter Sicherheitsmaßnahmen ist nur dann gegeben, wenn sie regelmäßig geprüft und kontinuierlich weiterentwickelt werden.

5 Inkrafttreten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen auf der Webseite der Hochschule in Kraft.

26.01.2022, Frankfurt am Main

Prof. Elmar Fulda, Präsident