Benutzung der ZMT IT-Infrastruktur

Netzwerkordner und Datensicherung

Im Windows Datei-Explorer sind bereits drei Netzlaufwerke verbunden:

Netzlaufwerk Y: "**Projects**"

Unter diesem Pfad liegen alle persönlichen Netzwerkfreigaben.

Netzlaufwerk Z: "**Home Drive**"

Dies ist der eigene, private Netzwerkordner „Z:"

Auf diesen Ordner hat ausschließlich der/die Anwendende selbst Zugriff, wichtige Dateien sollten in diesem Ordner gespeichert werden. Dateien welche hier gespeichert sind, werden in regelmäßigen Abständen mit in das Backup aufgenommen.

Dateien sollten niemals nur lokal auf einem Computer gespeichert werden.

Netzlaufwerk P: "**Public**"

Der „public" Netzwerkordner dient dem temporären Austausch von nicht sensiblen Dateien. Alle Kolleg*innen am ZMT haben Zugriff auf diesen Ordner, Dateien die hier abgelegt werden sind für jedermann sichtbar.
Dateien welche hier abgelegt werden, werden ohne Warnung nach fünf Tagen unwiederbringlich gelöscht.

ZMT cloud

Für den Austausch von Dateien mit externen Teilnehmenden steht eine Cloudlösung mit 25 GB Speicherplatz zur Verfügung.
Die Cloud erreicht man unter folgender Adresse im Browser:
https://zmtcloud.leibniz-zmt.de

Login mit ZMT-Account, der Name ist das dreistellige Userkürzel, das Passwort ist das des ZMT-Accounts.

Drucker (FindMe)

Am ZMT wird drucken über "FindMe" angeboten.
Alle Drucke werden grundsätzlich auf diesem Drucker gedruckt und unter Eingabe einer PIN am Gerät selbst abgeholt. Diese PIN findet sich in der Inbox des ZMT E-Mail Accounts.
Mit dieser PIN ist es möglich sich an den Geräten anzumelden um neben dem standardmäßigen drucken auch Funktionen wie "Scan to folder", "Scan to Mail" oder die Kopierfunktion zu nutzen.

ZMT E-Mail
Das ZMT stellt einen webbasierten Client zur Verwaltung von E-Mails zur Verfügung, dieser ist im Browser unter folgender Adresse abrufbar:
https://webmail.leibniz-zmt.de

Login mit vollständiger E-Mail Adresse und Accountpasswort:

BENUTZERNAME: vorname.nachname@leibniz-zmt.de
PASSWORT: siehe ZMT Accountformular

Alfresco (ZMT intranet)
Dieses System dient dem Austausch von organisatorischen Informationen und Dokumenten für das gesamte ZMT. Speziell die Arbeitsgruppen der Forschungsinfrastruktur stellen auf ihren „Sites" die verfügbaren Dienstleistungen vor. Alfresco erreicht man unter folgender Adresse im Browser:
https://intranet.leibniz-zmt.de

Login mit ZMT-Account, der Name ist das dreistellige Userkürzel, das Passwort ist das des ZMT-Accounts.

Knowledge Base
In der Knowledge Base des IT Helpdesk liegen bereits viele Hilfestellungen bereit. Dort finden sich Anleitungen zu vielen IT bezogenen Themen wie z.B.: der Bedienung des Videokonferenzsystems, der Einrichtung der Drucker und mehr. Dieser Bereich wird ständig aktualisiert und erweitert.
https://helpdesk.leibniz-zmt.de/help

Login mit ZMT-Account, der Name ist das dreistellige Userkürzel, das Passwort ist das des ZMT-Accounts.

ZMT IT Support (Helpdesk)
Bei Problemen mit einem ZMT-Gerät oder einer Anwendung, notwendigen Installationen von Programmen, oder zum Melden von Fehlern ist bitte das ZMT IT Helpdesk zu benutzen. Hierbei ist es wichtig, dass pro Ticket nur eine Anfrage gemeldet wird damit Tickets ordentlich an den/die zuständige/n Kolleg*in weitergeleitet werden können. Einzige Ausnahme ist das Melden von benötigten Softwareinstallationen oder Updates.
Das Helpdesk ist unter folgender Adresse erreichbar:
https://helpdesk.leibniz-zmt.de

Login mit ZMT-Account, der Name ist das dreistellige Userkürzel, das Passwort ist das des ZMT-Accounts.

Security Awareness Training (KnowBe4)
Alle Kolleg*innen erhalten regelmäßig Erinnerungsmails von KnowBe4 (do-not-reply@de.knowbe4.com) zu Schulungen.Es ist wichtig, dass diese Schulungen innerhalb der festgelegten Zeit absolviert werden.

Folgende Merkmale dieser E-Mails sind zu beachten:

- Absenderadresse: **do-not-reply@de.knowbe4.com**
- Sprachen: Deutsch und Englisch.
- Hinweis, nicht auf die E-Mail zu antworten.
- Aktuelle Standardsignatur des ZMT.
- Link für schnellen Login.

Diese Schulungen sind nicht nur ein wesentlicher Teil unserer Sicherheitsstrategie, sondern auch verpflichtend für alle Mitarbeiter.