Deutsches Zentrum
DLR für Luft- und Raumfahrt e.V.
in der Helmholtz-Gemeinschaft

Handout

IT security measures of the DLR

for the adoption of the regulations of the DLR IT security concept

Every employee and user (even external) of the DLR network is obliged to adhere to the following IT security measures. We do explicitly point out to the applicable company agreements of the DLR (e.g. concerning the usage of the WWW, etc.). The IT manager / IT security officer of the institute or facility is authorized to verify compliance with these IT security measures and to order measures for compliance with the IT security regulations of the DLR.

1. Network / Internet access

- The connection of private PC's or Laptops to the DLR network (even via VPN connections) is prohibited.
- When opening or downloading files users are responsible for ensuring all corresponding security guidelines are adhered to. The installation of unauthorized software is prohibited. If in doubt, authorization for the installation of software is to be requested from the IT security officer of the institute or facility.
- The use of communication or chat programs, with the exception of current DLR standard software, within the DLR network is prohibited. Software prohibited by this rule includes ICQ, Skype, AIM, Yahoo Messenger and Google Talk.

2. Workplace / Office

- To safeguard against unauthorized persons accessing hardware, the DLR network or confidential data password protected screen-savers or PC locks should be used.

3. Software / Anti-virus software

- As a basic principle only software approved by the IT manager of the institute or facility may be used. The installation of private software, also of either freeware or shareware, is only in exceptional cases permitted and requires the explicit permission of the IT manager of the institute or facility.
- Should a user find a computer to be infected with a virus the IT security officer, or IT manager of the institute or facility, should be informed immediately.

4. Hardware

- Should it be necessary for computer hardware to be serviced or repaired outside of DLR then all confidential and valuable data must be first secured and then deleted from the corresponding piece of hardware such that subsequent reconstruction of the data is impossible. In the case that this is not technically possible, the data storage device must be first removed from the device requiring repair. If the data storage device is damaged, it must be destroyed by an official data disposal company such that subsequent reconstruction of the data is impossible (See the IT manager or the IT security officer for support).
- All IT equipment (including such devices as PC's, PDA's, mobile phones, test-rigs, data-acquisition devices, IP-telephones, robots, work stations, etc.) no longer required, but containing valuable or important data, must be correctly disposed. This means that the data must be deleted, or the equipment destroyed, such that subsequent reconstruction of the data

Chief IT Security Officer of the DLR: Uwe Gorschütz (uwe.gorschuetz@dlr.de)

is impossible (See the IT manager or the IT security officer for support). The use of private IT equipment within the DLR network is prohibited.

- All auxiliary equipment, as well as all accessories, must be registered and approved. The person responsible for registration and approval is the IT manager of the institute or facility. The use of unapproved equipment is prohibited. The use of private auxiliary equipment and accessories is prohibited. Equipment prohibited by this rule includes USB devices such as USB flash drives and external USB hard drives.

5. Digital storage media

- Employees are responsible for the safe and proper use, and storage, of the digital storage media they use.
- Before transferring digital storage media to others it must be ensured that only the data intended for transfer is contained on the storage device.
- Every employee is responsible for ensuring that any information they forward will be received by authorized persons only.
- Storage devices are to be checked for viruses prior to forwarding to others. The sender of the storage device is responsible for ensuring the device is free from viruses.
- All electronic documents to which changes are not sought or intended are only to be made externally available in PDF format with write protection and, if applicable, copy protection.

6. Passwords

- We do explicitly point out to the applicable password policy of the DLR.
- A password should be at least 10 characters long, difficult to guess and contain at least 3 out of 4 characteristics (characteristics are upper case letters, lower case letters, digits, symbols).

I have taken notice of the IT security measures mentioned above.

Institute

SHRIYA HAZRA
Employee name

Shriya
Date / Signature

Deutsches Zentrum
DLR für Luft- und Raumfahrt e.V.
in der Helmholtz-Gemeinschaft

Handout

IT-Sicherheitsmaßnahmen des DLR

in Anwendung der Bestimmungen des DLR IT-Sicherheitskonzeptes

Jeder Nutzer (auch Externe) des DLR-Netzes sowie jeder Mitarbeiter (auch Externe) ist zur Einhaltung der folgenden IT-Sicherheitsmaßnahmen verpflichtet. Auf die entsprechenden Betriebsvereinbarungen (z.B. GBV zur Nutzung des WWW, etc.) wird ausdrücklich hingewiesen. Der IT-Manager / IT-Sicherheitsbeauftragte der Einrichtung oder der IT-Sicherheitsbeauftragte des DLR ist befugt, die Einhaltung dieser IT-Sicherheitsmaßnahmen zu überprüfen und geeignete Maßnahmen zur Einhaltung der IT-Sicherheitsbestimmungen des DLR anzuordnen.

1. Netzwerkzugriff / Internet

- Die Anbindung von IT-Geräten an das DLR-Netz (auch über VPDN), die nicht Eigentum oder Bestandteil eines Leasingvertrages des DLR sind, ist untersagt.
- Dienstliche Laptops sind mindestens einmal monatlich mit dem DLR-Netz zu verbinden. Somit wird der Softwarestand der Geräte rechtzeitig aktualisiert.
- Die Verwendung von Kommunikations- und Chat-Programmen (außer die geltenden Standards des DLR) innerhalb des DLR-Netzes ist untersagt. Dazu zählen unter anderem die bekanntesten Vertreter ICQ, Skype, AIM, Yahoo Messenger und Google Talk

2. Arbeitsplatz / Büro

- Bei Abwesenheit vom Arbeitsplatz ist mit Bildschirm- oder PC-Sperre sicherzustellen, dass Unbefugte keinen Zugang zu dem Endgerät, dem Netzwerk oder vertraulichen Daten haben.

3. Software / Virenschutz

- Grundsätzlich darf nur solche Software genutzt und installiert werden, die vom IT-Manager der Einrichtung freigegeben wurde. Die Installation von privater Software, auch von Free- und Shareware, ist nur in Ausnahmefällen gestattet und bedarf der gesonderten schriftlichen Genehmigung des IT-Managers der Einrichtung.
- Beim Auftreten eines Virus hat der betroffene Mitarbeiter umgehend den IT-Sicherheitsbeauftragten bzw. bei Nichterreichen den IT-Manager der Einrichtung zu verständigen.

4. Hardware

- Mobile Geräte (z.B. Laptops / Smartphones, Datenträger) sind stets besonders gesichert aufzubewahren und niemals an firmenfremde Personen weiterzugeben.
- Werden IT-Geräte außer Haus gewartet bzw. repariert, müssen sämtliche vertrauliche Daten gesichert und anschließend auf dem Gerät nicht-rekonstruierbar gelöscht werden. Falls dies aus technischen Gründen nicht möglich ist, muss der Datenträger ausgebaut werden.
- Alle IT-Geräte (dazu gehören u.a. PCs, PDAs, Mobiltelefone, Prüfstände, Messwerterfassungsplätze, IP-Telefone, Roboter, Workstations, etc.), die schützenswerte Daten enthalten und nicht mehr gebraucht werden / defekt sind, müssen ordnungsgemäß entsorgt werden. Dies bedeutet, dass die zu schützenden Daten so entfernt bzw. die Geräte so entsorgt (durch professionelle Entsorgungsfirmen) werden, dass eine Rekonstruktion der Daten nicht möglich ist.

IT-Sicherheitsbeauftragter des DLR: Dipl.-Ing. Uwe Gorschütz (uwe.gorschuetz@dlr.de)

Handout

- Alle Peripheriegeräte (auch ohne Netzzugriff) sowie sämtliches Zubehör müssen registriert und freigegeben werden. Zuständig hierfür ist der jeweilige IT-Manager der Einrichtung. Die Nutzung nicht freigegebener Geräte ist untersagt. Die Nutzung von privaten Peripheriegeräten und Zubehör ist untersagt. Dies gilt auch für USB Geräte sowie USB Sticks oder USB Festplatten.

5. Datenträger

- Mitarbeiter sind für die sichere, sachgerechte Nutzung und Lagerung der von ihnen genutzten Datenträger verantwortlich.
- Vor der Weitergabe eines Datenträgers ist sicherzustellen (z.B. durch vorheriges Entfernen der Daten, ohne Wiederherstellungsmöglichkeit), dass dieser nur die zur Weitergabe bestimmten Daten enthält.
- Jeder Mitarbeiter ist dafür verantwortlich, dass die von ihm weitergeleiteten Informationen nur an berechtigte Empfänger weitergegeben werden.
- Datenträger sind vor dem Versand grundsätzlich auf Viren zu prüfen. Der Versender des Datenträgers ist für die Virenfreiheit desselben verantwortlich.
- Alle elektronischen Dokumente, deren weitere Verarbeitung nicht gewünscht bzw. beabsichtigt ist, dürfen nur im PDF-Format mit Veränderungs- und ggf. Kopierschutz nach außen gegeben werden.

6. Passwörter

- Es gilt die Passwortrichtlinie des DLR in der gültigen Fassung.
- Ein Passwort sollte mindestens 10 Zeichen lang und nicht leicht zu erraten sein, aus Groß- und Kleinbuchstaben bestehen sowie mindestens eine Zahl bzw. ein Sonderzeichen enthalten.

7. Dienstreisen

- Bei der Dienstreise ins Ausland beachten Sie bitte das "Merkblatt für Dienstreisende ins Ausland"
- Melden Sie etwaige Kontrollen unmittelbar nach Ihrer Rückkehr dem IT-Sicherheitsbeauftragten des DLR sowie Ihrer Institutsleitung.

Ich habe die genannten IT-Sicherheitsmaßnahmen zur Kenntnis genommen.

RY-GNC HB
Institut

SHRIYA HAZRA
Mitarbeiter Name

Shriya
Datum / Unterschrift