Guidelines for the use of IT systems at DTU Compute

Scope and Background
These guidelines characterize what constitutes good behavior for users of IT systems at DTU Compute.

The guidelines cover the use of all IT systems provided by DTU Compute, and all IT systems that connect to or otherwise interact with or through DTU Compute's network, regardless of ownership or method of connection.

The IT systems include, but are not limited to, large and small computers, scanners, printers, PDAs, smart phones and other devices that can store or process information, regardless of the system's type or geographic location.

A user of IT at DTU Compute must comply with:

- DTU common rules for IT security (available on the intranet "Portalen"),
- these guidelines for the use of IT systems at DTU Compute,
- DTU Compute's rules on IT security, see intranet "Portalen" (under "DTU Compute / IT security"),

It is the user's responsibility to know the rules currently in force.

Approved use of IT systems
DTU Compute wants the security and reliability of the Department's IT systems to be as high as possible, and the department to be seen as having responsible and professional users of its IT systems.

The IT systems at DTU Compute should primarily be used for work purposes and users should be careful to ensure that the department is able to fulfil legal requirements, licensing obligations, etc. The IT systems must not be used in a way that could harm DTU's or DTU Compute's interests.

The user must ensure that the rules on IT security are respected and take note of of any breaches of security. User names and corresponding passwords are strictly personal and must be kept confidential. User identities are created, modified and deleted according to rules defined by the department management.

Users of specialized software must ensure that all licensing requirements are properly met.

IT systems are a limited and precious resource and the user must treat the IT systems with appropriate care.

E-mail and Documents
E-mail and other documents stored electronically, transmitted or received via DTU Computes IT systems shall be considered -- and treated in the same way -- as written communication. The user must therefore comply with the requirements for archiving, journalisation, etc. All e-mails must contain clear identification of the sender.

Data
Work-related data, including personal data, are often covered by legislation or agreements regarding their use and sharing/dissemination. The user must ensure that such laws and agreements are respected.

It is the user's responsibility to ensure that DTU Compute always has access to the latest version of work-related data, even without the employee's explicit involvement, unless there is a previously agreed exemption from this requirement. Access can be established by saving an unencrypted version of all data on the department's or DTU's servers or, should that not be possible, by depositing the encryption-key or credentials required to access accounts with external service providers.

Personal Use
DTU Compute's management allows limited use of the IT systems for the user's private purposes as long as this private use does not affect the user's work and takes place in accordance with any instructions given.

Personal webpages must not contain content that conflicts with DTU's general rules and guidelines. DTU Compute has formulated a set of specific rules, which include DTU's rules and which can be found on the Portal (under "DTU Compute / IT Security / Policies").

Monitoring, logging, penalties, etc..
Activity on DTU Compute's IT systems is automatically logged in order to monitor the systems' operation, maintain accounts of resource consumption and identify misuse. Collected information includes network traffic, senders and receivers of e-mails, identification of active users and information about print jobs.

If there is a suspicion of misuse, the director of the department has authorised the persons responsible for network security to monitor all activities, including inbound and outbound email without informing the user first.

Misuse and attempted misuse are considered as dereliction of duty, which may lead to disciplinary action after a comprehensive assessment of the scope and nature of the misuse and after consultation with the Human Resources Department.

Disciplinary action may consist of: a reprimand, formal warning, dismissal and, in the case of gross negligence, expulsion. Please refer to the Staff Handbook, available via the Portal (under "Employee").

Responsibilities
The Head of Department is ultimately responsible for all aspects of DTU Compute's IT systems and can resolve any questions about the use of IT.

Questions related to information security at DTU Compute should be addressed to the local IT Security Officer or DTU's IT Security Coordinator.

This is a translation of the guidelines approved by DTU Compute's management on 15th August 2017. Per B. Brockhoff, Head of Department.

I, the undersigned (name in block letters) _____
have read these guidelines, which apply to my use of DTU Compute's IT systems.

Date: Signature:

Guidelines for the use of IT systems at DTU Compute

Scope and Background
These guidelines characterize what constitutes good behavior for users of IT systems at DTU Compute.

The guidelines cover the use of all IT systems provided by DTU Compute, and all IT systems that connect to or otherwise interact with or through DTU Compute's network, regardless of ownership or method of connection.

The IT systems include, but are not limited to, large and small computers, scanners, printers, PDAs, smart phones and other devices that can store or process information, regardless of the system's type or geographic location.

A user of IT at DTU Compute must comply with:

- DTU common rules for IT security (available on the intranet "Portalen"),
- these guidelines for the use of IT systems at DTU Compute,
- DTU Compute's rules on IT security, see intranet "Portalen" (under "DTU Compute / IT security"),

It is the user's responsibility to know the rules currently in force.

Approved use of IT systems
DTU Compute wants the security and reliability of the Department's IT systems to be as high as possible, and the department to be seen as having responsible and professional users of its IT systems.

The IT systems at DTU Compute should primarily be used for work purposes and users should be careful to ensure that the department is able to fulfil legal requirements, licensing obligations, etc. The IT systems must not be used in a way that could harm DTU's or DTU Compute's interests.

The user must ensure that the rules on IT security are respected and take note of of any breaches of security. User names and corresponding passwords are strictly personal and must be kept confidential. User identities are created, modified and deleted according to rules defined by the department management.

Users of specialized software must ensure that all licensing requirements are properly met.

IT systems are a limited and precious resource and the user must treat the IT systems with appropriate care.

E-mail and Documents
E-mail and other documents stored electronically, transmitted or received via DTU Computes IT systems shall be considered -- and treated in the same way -- as written communication. The user must therefore comply with the requirements for archiving, journalisation, etc. All e-mails must contain clear identification of the sender.

Data
Work-related data, including personal data, are often covered by legislation or agreements regarding their use and sharing/dissemination. The user must ensure that such laws and agreements are respected.

It is the user's responsibility to ensure that DTU Compute always has access to the latest version of work-related data, even without the employee's explicit involvement, unless there is a previously agreed exemption from this requirement. Access can be established by saving an unencrypted version of all data on the department's or DTU's servers or, should that not be possible, by depositing the encryption-key or credentials required to access accounts with external service providers.

Personal Use
DTU Compute's management allows limited use of the IT systems for the user's private purposes as long as this private use does not affect the user's work and takes place in accordance with any instructions given.

Personal webpages must not contain content that conflicts with DTU's general rules and guidelines. DTU Compute has formulated a set of specific rules, which include DTU's rules and which can be found on the Portal (under "DTU Compute / IT Security / Policies").

Monitoring, logging, penalties, etc..
Activity on DTU Compute's IT systems is automatically logged in order to monitor the systems' operation, maintain accounts of resource consumption and identify misuse. Collected information includes network traffic, senders and receivers of e-mails, identification of active users and information about print jobs.

If there is a suspicion of misuse, the director of the department has authorised the persons responsible for network security to monitor all activities, including inbound and outbound email without informing the user first.

Misuse and attempted misuse are considered as dereliction of duty, which may lead to disciplinary action after a comprehensive assessment of the scope and nature of the misuse and after consultation with the Human Resources Department.

Disciplinary action may consist of: a reprimand, formal warning, dismissal and, in the case of gross negligence, expulsion. Please refer to the Staff Handbook, available via the Portal (under "Employee").

Responsibilities
The Head of Department is ultimately responsible for all aspects of DTU Compute's IT systems and can resolve any questions about the use of IT.

Questions related to information security at DTU Compute should be addressed to the local IT Security Officer or DTU's IT Security Coordinator.

This is a translation of the guidelines approved by DTU Compute's management on 15th August 2017. Per B. Brockhoff, Head of Department.

I, the undersigned (name in block letters) _____
have read these guidelines, which apply to my use of DTU Compute's IT systems.

Date: Signature: