Emergency Plan

Technical University of Denmark

May 2021

(For public use)

Emergency plan for DTU

Purpose

The purpose of the DTU emergency plan is to create a common framework for dealing with incidents which cannot be managed using normal resources and routines. The focus of the plan is to save lives and valuable property, protect DTU's reputation, continue the performance of DTU's core tasks, and restore operations at DTU after an incident.

DTU's emergency plan is part of DTU's strategy, and supports DTU's strategic aim of being a safe and secure university. DTU's emergency plan ensures active leadership in the event of an incident that could affect DTU as a whole, while ensuring the continuity of DTU's core operations.

This emergency plan is the general guiding document for emergency response work across DTU.

The emergency plan describes roles, responsibilities, and mandates in dealing with incidents at various crisis levels.

In addition, the Sustainability Policy for DTU's campus areas stipulates that DTU must work to protect the university from adverse incidents and build up capacity to implement remedial measures in the event of accidents, based on holistic emergency planning.

The Sustainability Policy also states that DTU must have a safety culture based on up-to-date risk assessments, plans, and procedures, which this emergency plan embodies.

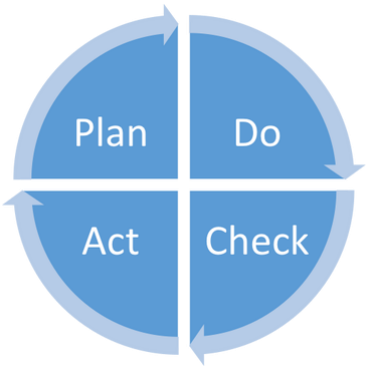
DTU's Information Security Policy (IT security) is supported by the emergency plan.

In addition, the emergency plan seeks to reflect selected targets of the UN Sustainable Development Goals in terms of creating a safe, non-violent, inclusive, and effective learning environment, and building up capacity and resilience.

Basis

DTU's preventive work with risks is based on risk assessments (e.g. ISO 31000 Enterprise Risk Management). DTU recognizes that not all risks can be prevented, and addresses this residual risk by having an emergency plan.

DTU's emergency plan is based on ISO 22301 (Business Continuity Management). In this context, the emergency plan encompasses essential aspects during and after an incident, and ensures the continued operation of critical functions and deliveries.



The methodology related to work with the emergency plan is based on the plan-do-check-act principle.

DTU's work with handling and preventing emergency incidents should therefore be seen as dynamic work that is continuously updated with adapted countermeasures.

Explanation of terms

Executive Board	President and other members of the Executive Board.
Unit leader	'Unit leader' is DTU's term for what is called 'sector leader' in government and emergency response terminology. Being a unit leader means that the responsibility a person has in their unit during normal operation is retained during an incident.
Corporate staff	The term 'corporate staff' covers DTU's administrative units (AFRI, APR, AKM, AIT, AUS, AØR, CAS, and AHR). There is a description of corporate staff on DTU's website.
Corporate emergency response team	The corporate emergency response team consists of the CAS director of facilities, CAS operations manager, CAS AB head of section, and CAS AB emergency managers.
Crisis management organization	The crisis management organization is defined as the relevant unit leaders who are activated to handle a specific incident.
Staff function	The term 'staff function' covers an area of activity of corporate staff.
University unit	The term 'university unit' is used in the emergency plan as a single term to encompass departments, centres, and corporate staff.

Scope

The emergency plan applies to DTU's entire organization - i.e. all employees and students, irrespective of their location in their DTU activities.

Employees and students who happen to be on location at other organizations must generally follow the local instructions that apply at the relevant location. However, in special cases, DTU's emergency plan can activate measures that go beyond the local instructions and which employees and students must therefore comply with.

The emergency plan applies to all external partners and visitors present on DTU properties.

Tenants are generally covered by the emergency plan in relation to the rented premises.

DTU's collaborative partners and local community can apply for support from DTU in relation to handling incidents.

How the emergency plan interfaces with the OHS legislation

As part of the risk assessment process for their own work, university units must prepare risk assessments in line with the OHS legislation. The risk assessment will typically be at object level and for execution of the work—such as a test setup, work with chemicals, etc. This risk assessment must state what will be done in the event of an incident. This is referred to as an 'emergency plan' in OHS legislation and must not be confused with this emergency plan. The

section of the risk assessment covering what to do in the event of an incident must not conflict with DTU's emergency plan.

How the emergency plan interfaces with IT security
IT has several roles in the emergency response context. In relation to its own unit, where incidents occur and are handled, and in the context of other entities.

How IT incidents are handled at DTU as an organization has a major impact on DTU's finances, reputation, and ability to perform its activities. IT is also an important tool in emergency response work in almost every other conceivable incident.

DTU uses ISO 27001 (Information Security) as the guiding structure for work on information security - including for the IT security related emergency response work that is an integral part of the standard.

Information security is implemented at DTU in the existing management hierarchy. Each unit has full responsibility for information security in its own unit. This also applies to the handling of local incidents, which are handled on the basis of the unit's own risk assessment.

Common DTU procedures have been prepared for IT security - for incident management, risk assessment etc., and this is carried out within the unit and can be escalated.

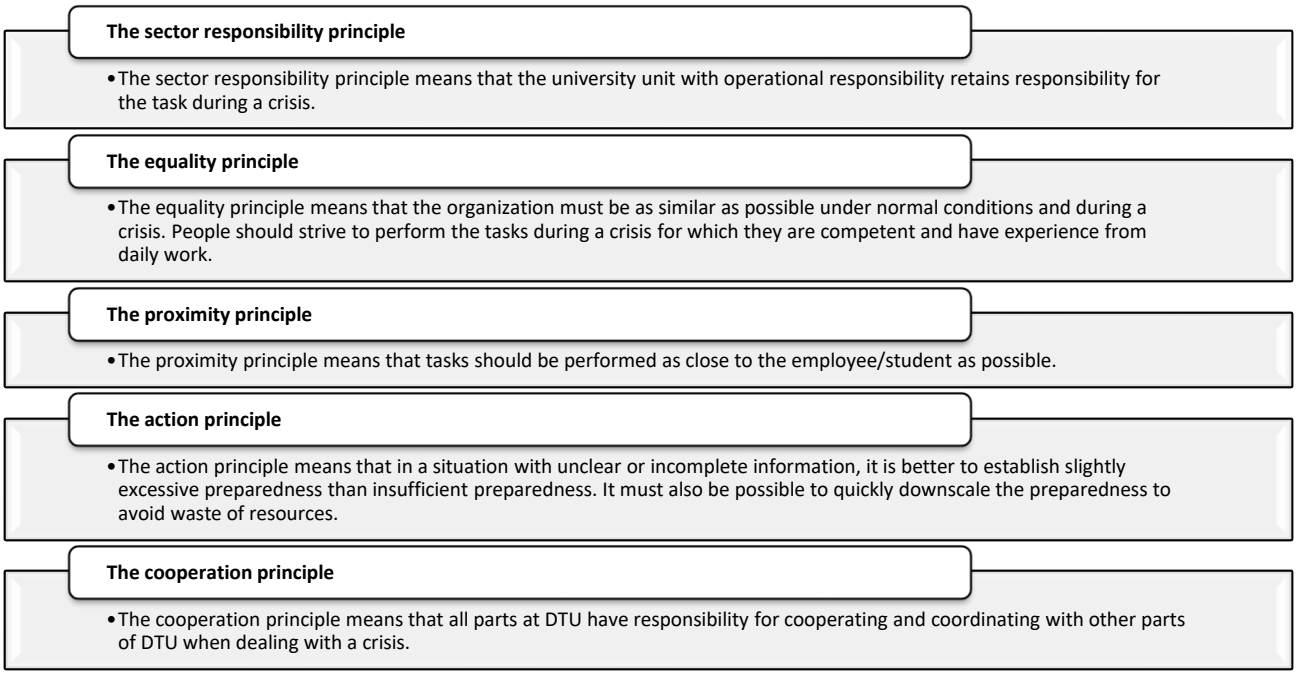
Updates and availability

DTU's corporate emergency management is responsible for preparing and updating this emergency plan, so that it is always up-to-date. Changes to the emergency plan must be approved by the Executive Board, while minor adjustments can be made without board approval.

The emergency plan and underlying documents must be stored on a central dedicated platform, which is always available to unit leaders and other relevant internal actors. The emergency plan must always be accessible via a common digital entry point. An up-to-date hardcopy version of the emergency plan must also be available in the president's office and in CAS.

Basic principles

DTU's preparedness is rooted in the following principles:



Crisis levels

This section is not publicly available

Documentation

It is important to ensure thorough documentation in relation to an incident. All actors are responsible for ensuring that as much documentation as possible is collected—as soon as possible. Documentation should be collected throughout the incident to ensure complete documentation is available.

To support the documentation, a log can be kept of the course of events during a crisis. All actions and enquiries should be logged by the person who receives the information. It is important that DTU can go back to the log at any time and see what has been done and who DTU has been in contact with. This is particularly important in relation to handling the media and any follow-up by the authorities, insurance etc.

The documentation must be recorded with due respect to any injured persons, and be handled in line with the rules for personal data and privacy.

Reporting injuries and near-misses

All incidents affecting employees or students, where personal injury has or could have occurred, must be reported via DTU Injury, so that the OHS organization can follow up on the incident. An incident that could have resulted in personal injury must be recorded as a *near-miss incident*.

External partners who perform work for DTU must inform the assigned contact person at DTU in the event of personal injury or a *near-miss incident,* and the incident must be recorded in DTU Injury.

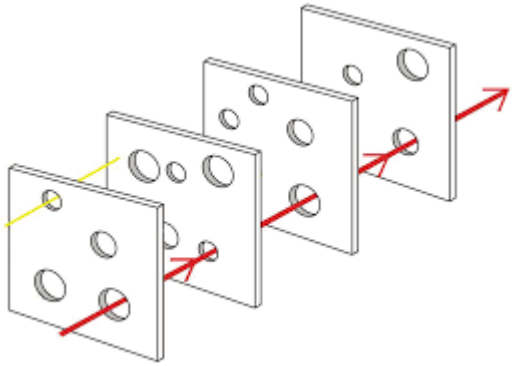
Reporting IT incidents
IT security incidents are reported and handled in line with DTU's 'Incident reporting procedure'.

Incident reporting is also an integral part of the organizational and management orientation.

Incident handling evaluation

Every incident is evaluated afterwards. The purpose of the evaluation is collect data that can support DTU's incident management in relation to this emergency plan.

The evaluation should always start by identifying the countermeasures (barriers) that were unable to prevent the given incident. The Swiss cheese model, for example, can be used. The principle of the model is that countermeasures must have been broken for the incident to unfold.



After the relevant barriers have been identified, the issues are referred to the people responsible for these. On this basis, existing countermeasures can be reinforced, or new countermeasures can be put in place, to counteract future incidents.

The process of handling the incident should then be evaluated. The following three points should be covered in the evaluation as a minimum:

- What worked well during the given incident and should therefore be retained?
- What was less than ideal and should therefore be adjusted?
- What points of attention or problems arose along the way?

Evaluation of the specific incident is anchored with the relevant management, drawing on the relevant actors, and aims to ensure that the necessary actions are taken in relation to countermeasures at DTU.

Competences

Unit leaders must ensure that relevant employees have the competences necessary to perform their emergency response task within the unit's area of responsibility.

To ensure that competences relevant to emergency response are retained, developed, and maintained, unit leaders should continually and systematically consider four questions:

- What competences does the unit need to have?
- Which people should be trained?
- How should competence development take place?
- How should competences be maintained?

Structure of the plan

The emergency plan is divided into four main sections:

- *Plan for acute handling (seconds/minutes)* describes how an emergency response incident should be handled here and now by the person on the scene observing the incident.
- *Plan for crisis management and crisis communication (hours/days)* describes the crisis management organization and its functioning—including principles for crisis communication.
- *Business continuity plan (hours/days)* describes how to maintain operation of critical functions and deliveries.
- *Plan for recovery (indefinite)* describes how to organize the work towards normalizing operations.

The structure of the emergency plan reflects the order in which the different phases of handling an incident occur. This is illustrated in the figure below.

PLAN FOR ACUTE HANDLING

This section describes DTU's plan for the acute handling of an incident during the first seconds/minutes. It describes which actions the person observing the incident should perform.

Activation

Everyone (employees, students, visitors, tenants, external partners, etc.) has an obligation to activate a given emergency response instruction.

Roles and responsibilities

Employees, students, visitors, tenants, etc. are responsible for initiating handling of an incident—this includes commencing DTU's evacuation procedure, attempting to mitigate the incident, and if possible, stopping the spread of the incident.

Everyone is also obligated to take action in response to events or situations where the safety of people, valuable property or the environment could be compromised.

Emergency instructions

DTU has prepared general emergency instructions for dealing with a number of serious incidents. General emergency instructions are available for:

- Fire
- Serious injury
- Critical building damage
- Serious IT security Incidents
- Personal data breaches
- Threats
- Unstable chemicals
- Radioactive leak
- Suspicious objects
- Active Shooter

The university units must be familiar with the emergency instructions, and the local management must decide whether to adapt the instructions to local conditions.

Evacuation procedure

DTU has a common procedure for evacuating buildings. However, evacuation may be different in certain cases where special circumstances apply. Instructions on this should be given locally. It is a local responsibility to ensure that the evacuation procedure is rehearsed.

PLAN FOR CRISIS MANAGEMENT AND COMMUNICATION

This section of the plan describes how to activate the crisis management organization in the case of an incident, and the framework for the work and crisis communication of crisis staff.

Activation

This section is not publicly available

Roles and responsibilities

This section is not publicly available

Mandate

This section is not publicly available

Crisis communication

This section is not publicly available

Principles for crisis communication

This section is not publicly available

Internal and external communication

This section is not publicly available

Communication channels

This section is not publicly available

Principles for handling an event

This section is not publicly available

Crisis staff

This section is not publicly available

Task force

This section is not publicly available

Pandora cell

This section is not publicly available

Meeting place for crisis staff

This section is not publicly available

Agenda for crisis staff meetings

This section is not publicly available

BUSINESS CONTINUITY PLAN

Once the acute phase of the incident has been managed, special measures may be needed to continue operation of critical functions and deliveries at DTU. This is described in business continuity plans.

Activation

This section is not publicly available

Roles and responsibilities

This section is not publicly available

PLAN FOR RECOVERY

The aim of the recovery plan is to return DTU to normal operation after an incident.

The recovery plan applies to physical elements (hardware, buildings, outdoor areas, infrastructure, etc.), intangible elements (software, communication, etc.), and mental recovery in people.

Activation

This section is not publicly available

Roles and responsibilities

This section is not publicly available

CONTACT INFORMATION

This section is not publicly available