FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

January 2019
– 8/2018

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

# The protection of research data at the Danish universities

# 1. Introduction and conclusion

## 1.1. Purpose and conclusion

1. This report concerns protection of research data within the remit of the Ministry of Higher Education and Science. This ministry has the overall responsibility for research carried out at the eight Danish universities and allocated just under DKK 9 billion for research in 2018. Each individual university is responsible for ensuring a high level of local IT security in order to protect research data. The study was initiated by Rigsrevisionen in February 2018 and is based on IT audits carried out by Rigsrevisionen during the course of 2018.

2. The research data held by the universities are of great value and therefore obvious targets of cyber attacks or cyber espionage. In the past years, there have been several incidents of cyber attacks against Danish universities; in the spring 2018, it came to light that three Danish universities had been hacked in the period from 2014 to 2016 as part of a large global cyber attack launched by a foreign state actor. Threat assessments carried out by the Danish Centre for Cyber Security in December 2016 and in March 2018 lead them to conclude that the threat level towards Danish universities is high. Universities as well as public research environments are traditionally very open, which makes research data vulnerable to cyber attacks. According to the Centre for Cyber Security, research data in the fields of, for instance, economics, chemistry, physics, geology, environmental science and transport attract the attention of hackers. Research at the universities are funded partly by the Danish government, as mentioned above, and partly by the European Community and private partners, who contributed just under DKK 8 billion in 2018. It could therefore have financial consequences for the universities, if research data are copied or disappear. Such incidents may also weaken confidence in the affected universities, which can have serious consequences, because the universities depend on their ability to attract researchers and private research funding.

**The Danish Centre for Cyber Security**
The Danish Centre for Cyber Security is part of the Danish Defence Intelligence Service under the Danish Ministry of Defence. The purpose of the security authority is to assist Danish authorities and businesses in preventing, mitigating and protecting themselves against cyber attacks from foreign states.

3. The high threat level makes it important for the universities to maintain a high level of IT-security so as to protect research data.

The purpose of the study is therefore to assess whether the universities adequately protect research data.

Initially, we mapped the risk profiles of the five largest Danish universities in relation to their protection of research data against unknown IT equipment. Then we dug deeper at the largest university – the University of Copenhagen – to determine how the centralised IT department at the university and three selected departments work with IT security in relation to protection of research data.

## Conclusion

**IT equipment**
In the report, the term IT equipment refers to hardware on which software is installed.

**Unknown IT equipment**
This is equipment that the IT department has no records of in its system. Researchers may, for instance, bring their own devices and connect them to the university network without informing the IT department.

It is Rigsrevisionen's assessment that the five largest universities are not adequately protecting their research data against unknown IT equipment. As a result, foreign actors may relatively easy gain unauthorized access to the universities' research data. This is not considered satisfactory by Rigsrevisionen.

The Ministry of Higher Education and Research agrees that it is important for the universities to maintain a high level of IT security to protect research data. The ministry shares Rigsrevisionen's assessment that, despite the current focus on the area, there is potential and need for improvement.

The study shows that the five largest universities have defined guidelines for researchers' use of software and hardware centrally, but that they have failed to centralise efforts to maintain a satisfactory level of security for research data. This is due mainly to the fact that, at some universities, researchers are allowed to bring their own devices, and at all the universities, researchers are allowed to have local administrator privileges, which gives them access to install software. Additionally, all five universities know of incidents where unknown hardware has been connected to their network.

Overall, the centralised level of protection of research data against unknown IT equipment at the universities does not seem to be high, and Rigsrevisionen has therefore examined how one university - using the University of Copenhagen as an example - protects research data, both centrally and at three selected departments: The Department of Biomedical Science, the Department of Nordic Studies and Linguistics and the Niels Bohr Institute.

**ISO 27001**
The international information security standard that all government institutions have been required to follow since January 2014 and have fully implemented at the beginning of 2016. Independent public institutions are not required to follow ISO 27001, but the five largest universities in Denmark have decided to do so.

The study shows that the University of Copenhagen does not adequately protect research data. The university has decided to adhere to ISO 27001, but has not carried out a threat or risk assessment as prescribed in ISO 27001. Moreover, the management of the University of Copenhagen has only defined an inadequate general framework for the use and management of IT equipment at the university. Additionally, the management of the university has developed two policies that in practice leave the responsibility for IT security and the protection of research data to the individual researcher, who, in order to solve this task, must have insight in a number of the university's IT-security measures that are not described in the provided general framework. This approach has significantly limited the possibilities of establishing a high level of IT-security.

The review of IT security at the three departments shows that the task of protecting research data is not always solved locally. The Niels Bohr Institute has implemented a more advanced IT-security policy that may serve as inspiration for others, albeit it also has room for improvement. The remaining two departments have done nothing to improve security and are both under the impression that IT-security issues are solved centrally.

The management of the University of Copenhagen expects the researchers to take responsibility for storing research data, and Rigsrevisionen has therefore examined whether the researchers are familiar with and follow existing rules to protect research data in the best possible way. The study shows that only one of the 26 interviewed researchers was familiar with the university's guidelines on data protection. The study shows examples of researchers who store data in other and less secure ways than those provided by the university.

**The management of the University of Copenhagen**
The management refers to the executive management level of the university, including the rector of the university, pro-rector/provost and university director.

Rigsrevisionen notes that several of these issues have been brought to the attention of the management of the University of Copenhagen, but that no specific steps have been taken to secure an adequate level of IT security.

The Ministry of Further Education and Research has informed Rigsrevisionen that the department intends to ask the universities to identify and remedy any critical IT security breaches. The department will also work with the universities to produce a plan to establish the required IT security organisation and culture at the universities. The department further intends to launch a similar process at the other institutions of higher education.