Dear College van Bestuur, Dear Geert, Karen & Jan,

During the plenary meeting on the 22nd of February 2021 the Central Student Council (hereafter: CSR) has consented to your request for consent on the Principes voor informatiebeveiliging en het Autorisatiebeleid (your reference: 2020-135165).

The Central Student Council is very pleased that the unwritten rules of information security are being embedded via these policy documents. Unfortunately, the events of last week made it painfully clear why such principles are essential. That being said, we still have several recommendations to make these policy documents.

**Information principles**

Considering the first principle of proportionality, we recommend that the Board of Directors (CvB) handle a very low-risk appetite. Cybersecurity might not be one of the most alluring business operations subjects, but it becomes more critical every year. The CSR is aware that there is always a trade-off between openness and security; however, we also have to keep in mind that the consequences of data breaches or cybercrime can be immense for an institution as the UvA.

Furthermore, the policy documents state that the boundaries of the organisation are blurring. A lot of the ICT products are outsourced to third parties. We understand that such is necessary and how it creates a possible weakness in the University’s information security. Therefore, the CSR advises the CvB to follow rigorous procurement requirements while handling new tenders.

In addition to applying these principles to new tenders, we also trust that the current infrastructure will be revised to meet the requirements that follow the information security principles.
In order to further improve the cybersecurity at the UvA, the CSR recommends the CvB to organise hackathons once every year. Other institutions organise these as well. They are cost-efficient and will allow us to critically engage with the brilliant minds that make up our University’s student population. At the same time, it would aid in increasing the University’s security.

**Authorisation policy**

Regarding the authorisation policy, the CSR advises on three matters. Firstly, we would appreciate it if the RLWW (password policy) was updated. As we know, the complexity of a password does not necessarily improve the security against being hacked. The only thing that helps is the password’s length. Therefore, the CSR would like to see the minimal length of a password to be increased.

Secondly, the CSR advises against the use of biometric identifications. The latter does not follow the proportionality principle, and it is impossible to encrypt biometric identifications safely. Additionally, the CSR is not pleased with biometric identifications being used at USC locations. We are aware that they form their own legal entity. However, we hope the CvB agrees with us on this topic and proceeds to facilitate a discussion with the relevant parties regarding this.

Thirdly, the CSR recommends the CvB to discontinue the two-step verification via SMS. The latter is prone to fraud via SIM swapping. The advice the CvB to replace this two-step verification system via SMS and replace it with a safer and more secure one, preferably a two-step verification system via tokens.

Finally, the CSR is concerned about the lack of awareness amongst students and staff regarding updating their software promptly. We realise that this might not directly be within the scope of these policy documents; nevertheless, it is an important and relevant topic. Updating our software is the easiest way to stay protected from cybercriminals. Lagging on software updates makes it easier for hackers to penetrate a secure environment. Therefore, the CSR asks the CvB to raise more awareness on this topic.

The Central Student Council realises the importance of Information Security Policies, especially in the light of recent events. We are looking forward to helping whenever necessary regarding the recommendations mentioned above.

Met vriendelijke groet,

Nina Hol
Voorzitter CSR 20|21

~