Gebruik van IT-middelen die aan personeelsleden van Aedes zijn toevertrouwd

Wat zijn de doelstellingen van deze nota ?

- Gedragsregels vaststellen voor het gebruik van IT-middelen door Aedes-personeelsleden ;
- De personeelsleden ervan in kennis stellen dat hun IT-middelen zo nodig kunnen worden gecontroleerd en onderzocht.

Wat zijn de rechtsgrondslagen ?

- De AVG (GDPR) ;
- Het Belgische Arbeidsrecht ;
- Het Aedes arbeidsreglement.

Wat zijn « IT-middelen » ?

IT-middelen omvatten **hardware** (pc, tablet, smartphone) en **software** die door Aedes aan personeelsleden ter beschikking wordt gesteld voor de uitvoering van hun taken binnen het bedrijf.

Wat zijn de gedragsregels ?

1. Een « schoon » bureau

- Waanneer u het kantoor aan het eind van de dag verlaat, laat dan geen documenten met gevoelige informatie.
- Als de laptop de nacht op kantoor doorbrengt, zorg er dan voor dat u zich afmeldt (log off) voordat u het in slaapstand zet.

2. IT-middelen VOOR Aedes

- Wat door Aedes wordt toevertrouwd, mag uitsluitend worden gebruikt voor doeleinden die verband houden met de activiteiten van Aedes.

3. Hoe zit het met privégebruik ?

- Het is mogelijk de IT-middelen voor privédoeleinden te gebruiken en er tegelijkertijd voor te zorgen dat dit de uitvoering van de werkzaamheden niet hindert en andere gebruikers niet stoort.

4. Identificatiegegevens (login en paswoord) worden niet gedeeld

- Niets meer aan toe te voegen !

5. In geval van incident, is er maar één contactpunt

- Indien de identificatiegegevens gecompromitteerd lijken te zijn of in geval van een incident (diefstal/verlies van materiaal, hacking, …), dient u onmiddellijk een e-mail te sturen naar privacy@aedesgroup.be.

SA Aedes
Route des Canons, 3
5000 – Namur

Tél. +32 81 74 68 46
Fax +32 81 73 04 87
info@aedesgroup.be

RPM Liège, division Namur
BE 0460.855.809
www.aedesgroup.be

6. Wat privé is, blijft PRIVÉ

- Alle privédocumenten moeten in een "PRIVÉ"-bestand worden opgeborgen. In theorie kan het professionele e-mailadres (@aedesgroup.be) niet voor privédoeleinden worden gebruikt. Mocht dit toch het geval zijn, dan moet de titel van elke privé e-mail "PRIVÉ" luiden.
- Bovendien mag geen enkele professionele inhoud in een privé e-mail of -document worden geplaatst.
- Elk personeelslid is zich ervan bewust dat de opslag van privébestand te allen tijde verloren kan gaan/verwijderd kan worden (bijv. ontslag, IT-onderhoud, IT-beveiliging) en dat deze bestanden in geval van toezicht/onderzoek onderzocht kan worden. De gebruiker is dus als enige verantwoordelijk voor de back-up van deze privé-items.

7. In geval van afwezigheid…

- Een automatisch afwezigheidsbericht moet door de gebruiker worden ingesteld, of zal voor de gebruiker worden ingesteld in geval van een onverwachte afwezigheid.

8. Pas op voor phishing !

- Vreemde domeinnamen, zinnen met spelfouten, ongewone verzoeken... Druk nooit op een knop of download nooit een bijlage in een e-mail die er frauduleus uitziet. In het algemeen, open alleen de bestanden die je verwachtte. Elke bijlage die ongewoon is, moet verboden worden.

9. Ten slotte, is het verboden om…

- Vertrouwelijke, interne of geheime gegevens/informatie te verspreiden onder onbevoegde derden (of gebruikers), tenzij de direct leidinggevende hiervoor vooraf toestemming heeft gegeven ;
- Door intellectuele eigendomswetten of -rechten beschermde gegevens te verspreiden, te downloaden of op te slaan, in strijd met dergelijke wetten of rechten ;
- Aan een bijkomstige of ondersteunende beroepsactiviteiten deel te nemen;
- Op een ongeoorloofde manier persoonsgegevens van personeelsleden, makelaars, verzekerde, partners van Aedes of derden op te slaan of te verwerken ;
- Om inhoud te bekijken, op te slaan of te verspreiden die discriminerend, kwetsend, beledigend, racistisch, pornografisch, lasterlijk, moreel of seksueel intimiderend is, of enige andere vorm van onwettig of illegaal gebruik bevat ;
- Aan kettingbrieven of spam deel te nemen.

Waarom en wanneer moet een onderzoek worden ingesteld ?

Het bestuur kan door middel van gedocumenteerde instructies toestemming geven voor een onderzoek :

- in geval van een daadwerkelijk of vermoedelijk incident, of
- tegen een bepaalde gebruiker wanneer er een met bewijzen gestaafd vermoeden bestaat, of
- zoals vereist door de wet, een rechtbank of een bevoegde autoriteit.

Indien het onderzoek ongeoorloofd of onwettig gebruik van IT-middelen aan het licht brengt, behoudt Aedes zich het recht voor :

- disciplinaire maatregelen nemen tegen de betrokken gebruikers ;
- gerechtelijke stappen of procedures (met inbegrip van strafrechtelijke procedures) tegen de betrokken gebruikers te ondernemen.

SA Aedes
Route des Canons, 3
5000 – Namur

Tél. +32 81 74 68 46
Fax +32 81 73 04 87
info@aedesgroup.be

RPM Liège, division Namur
BE 0460.855.809
www.aedesgroup.be