Beleid BYOD (Bring Your Own Device) voor actieve leden

Actieve leden maken gebruik van eigen apparatuur, zoals telefoon, laptop of tablet, om werkzaamheden voor Partij voor de Dieren uit te voeren. Hiervoor gelden de volgende regels:

Het actieve lid:

1. dient de eigen apparatuur te beveiliging door middel van automatische vergrendeling en een pincode of wachtwoord waarbij het volgende advies wordt opgevolgd: Een sterk wachtwoord maken (externe website - Microsoft);
2. zorgt dat de software van de eigen apparatuur up-to-date is;
3. zorgt dat de eigen apparatuur versleuteld[1] is;
4. zorgt dat op de eigen apparatuur antimalwaresoftware actief is;
5. maakt zoveel mogelijk gebruik van tweestapsverificatie;
6. slaat informatie die behoort tot de organisatie alleen op in een beveiligde cloud-omgeving die door de organisatie wordt aangeboden;
7. zorgt dat anderen (waaronder huisgenoten) geen toegang hebben tot de informatie van de organisatie;
8. zorgt ervoor dat anderen bij vertrouwelijke informatie niet over de schouders kunnen meekijken of meeluisteren;
9. geeft (een vermoeden van) een hack of verlies, of enige andere aantasting van het apparaat direct door aan het partijbureau.
10. is zelf verantwoordelijk voor het veilig maken en houden van eigen apparatuur.

[1] Apparaten beveiligen via versleuteling is uitgebreider dan wanneer een het toestel enkel beveiligd wordt met een toegangscode bij het vergrendelingscherm. Zowel Android-telefoons als iPhones zijn tegenwoordig bijna altijd standaard versleuteld. Op internet is terug te vinden of de software van jouw type apparaat standaard versleuteld is en zo niet, hoe dit ingesteld kan worden. Gebruik zoektermen als ‘apparaatversleuteling windows’ of ‘versleutelen Adroid/apple telefoon’ om dit te achterhalen.