11 basismaatregelen om je informatie-beveiliging te verhogen

Bescherm je school tegen cyberaanvallen en verhoog de informatiebeveiliging met deze 11 basismaatregelen. Elke maatregel vermindert meteen hoge veiligheidsrisico's en digitale incidenten. Ze gelden zowel voor je eigen systemen als voor systemen van leveranciers.

De basismaatregelen zijn niet geordend op belangrijkheid of eenvoud. Het zijn geen *quick wins* en vragen om een tijdsinvestering en zorgvuldige implementatie. Om je hierbij te helpen, vind je bij iedere basismaatregel informatie en, indien beschikbaar, handreikingen en praktische ondersteuning. Soms vind je verwijzingen naar voorbeelddocumenten en bronnen uit andere sectoren die ook bruikbaar zijn voor het primair en voortgezet onderwijs.

Wie moet aan de slag met deze basismaatregelen?
Dit document is voor IBP'ers en medewerkers in het po en vo die verantwoordelijk zijn voor de informatiebeveiliging binnen hun school. Soms werkt je school met een externe (ict-)leverancier, die deze maatregelen moet treffen. Controleer altijd of dit is gebeurd. Het is aan te raden om met je schoolbestuurder, schoolleider en collega's in gesprek te gaan over de basismaatregelen om het bewustzijn binnen de school te vergroten.

Hoe gebruik ik deze basismaatregelen?
Met deze basismaatregelen zet je eerste concrete stappen om jouw school digitaal veiliger te maken. Bij elke maatregel vind je verschillende verwijzingen naar bronnen. De bronnen hebben meerdere functies:

1. Een bron kan meer informatie bevatten over het onderwerp.
2. Een bron kan een handreiking bieden hoe de maatregel geïmplementeerd kan worden.
3. Een bron verwijst naar een voorbeeld van een mogelijke aanpak voor de implementatie uit een andere sector.

Door wie worden deze maatregelen ondersteund?
De basismaatregelen worden aangeraden door het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center en sterk geadviseerd door het programma Digitaal Veilig Onderwijs.

Hoe verhouden deze basismaatregelen zich tot het Normenkader IBP FO?
Het Normenkader IBP FO is voor jou en jouw bestuur de leidraad voor een veilig digitaal onderwijs. Iedere basismaatregel is vereist binnen een of meerdere normen uit het Normenkader IBP FO. Zo dragen deze basismaatregelen bij aan het voldoen aan een deel van enkele normen. Daarom staan bij de basismaatregelen de normen genoemd waarmee een relatie is.

LET OP: Met het nemen van deze maatregelen voldoe je niet meteen aan de hele norm die erbij staat. Gebruik het Normenkader IBP FO om de normen te bekijken en toe te passen.

Hoe verhouden deze basismaatregelen zich tot het groeipad in het Normenkader IBP FO?
Deze basismaatregelen zijn een voorloper op het groeipad. Vanaf de tweede helft van 2024 word je met een logisch en volledig groeipad, inclusief daarbij passend ondersteuningsaanbod, stap voor stap meegenomen door het Normenkader IBP FO.

Hoe verhouden deze basismaatregelen zich tot de hulpmiddelen op de Aanpak IBP?
Kennisnet, een van de samenwerkingspartners binnen het programma Digitaal Veilig Onderwijs, ontwikkelt nieuw ondersteuningsaanbod en publiceert dit op de website 'Aanpak IBP'. Daarom vind je voor sommige van deze basismaatregelen verwijzingen naar handreikingen of hulpmiddelen op de Aanpak IBP.

Betrouwbare informatiebronnen
Meer betrouwbare Nederlandstalige informatie over cybersecurity vind je op:

- Aanpak IBP
- NCSC
- Informatiebeveiligingsdienst
- Security Expertise Centrum
- Digital Trust Center

Met het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken. Het programma biedt schoolbesturen heldere leidraden en een concreet ondersteuningsaanbod. Het programma stimuleert ook dat leveranciers hun productportfolio in lijn brengen met het normenkader. Zo kunnen scholen voldoen aan hun verantwoordelijkheid om een digitaal veilige organisatie te realiseren. Stap voor stap, Bit by Bit.

VO RAAD Vereniging van scholen in het voortgezet onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Kennisnet
PO RAAD
SIVON

1 Breng je applicaties en omgevingen in kaart (zeker waar persoonsgegevens in staan), leg contact met de interne en externe verantwoordelijke personen hiervoor vast en richt een proces in voor 'wat nou als het fout gaat'

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 2.1 5.2 9.1 14.1 14.2 15.3

- Inzicht in het applicatie-landschap
- Factsheet configuratie-management
- Hulpmiddelen 14. Bedrijfs-continuiteits-management
- Hulpmiddelen 15. Ketenbeheer

2 Maak afspraken met leveranciers

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 15.1 15.2 15.3 15.4

- Verwerkers-overeenkomsten
- Factsheet 5 Adviezen voor veilig inkopen van cloud-diensten
- Dienst Verwerkers-overeenkomsten

3 Richt risicomanagement in

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 3.1 3.2 3.3

- Risicoanalyse
- Handreiking risicomanage-ment door lijn-managers
- Factsheet risico-beheersing
- Richt risico-management in

4 Bepaal wie toegang heeft tot uw data en diensten en zorg dat het uitlegbaar is waarom personen toegang moeten hebben

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 4.4 10.1 10.2 10.5

- Bepaal wie toegang heeft tot uw data en diensten
- Beleid logisch toegangs-beveiliging
- Toegangsbeleid
- Beleid voor Identity Access Management

5 Beperk het aanvalsoppervlak

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 11.1 11.11 11.12

- Hardening beleid voor gemeenten
- Netwerk segmentering
- Beperk het aanvals-oppervlak

6 -11 >>

VO RAAD Vereniging van scholen in het voortgezet onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Kennisnet
PO RAAD
SIVON

6 Versleutel opslagmedia met gevoelige bedrijfsinformatie van belangrijke bedrijfsgegevens en privacygevoelige gegevens

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 9.3 9.4 11.3

Mobiele gegevens-dragers

Gebruik versleuteling

7 Bescherm uw organisatie tegen het verlies van gegevens door regelmatig back-ups te maken en te testen

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 13.1 13.2 14.3

Pas sterke authenticatie toe

Mobiele gegevens-dragers

Wachtwoord-beleid

8 Gebruik antivirus-software

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 11.12

Voorkom virussen en andere malware

9 Pas multifactor-authenticatie toe op de kritieke systemen

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 11.2

Pas sterke authenticatie toe

Handreiking 2 Factor authenti-catie (2FA) voor gemeenten

Wachtwoord-beleid

10 Centraliseer en analyseer loginformatie

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 10.1 11.4

Centraliseer en analyseer loginformatie

11 Installeer tijdig en op een gestructureerde manier updates

DEZE MAATREGEL HEEFT EEN RELATIE MET NORM: 5.2

Richt patch-management in

Factsheet patch-management

Patchmanage-ment voor gemeenten

<< 1 - 5

VO RAAD Vereniging van scholen in het voortgezet onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Kennisnet
PO RAAD
SIVON