Risico-analyse IBP

Kans: kans van het optreden van het risico

1. Klein: kan minder dan jaarlijks voorkomen
2. Middel: kan meerdere keren per jaar voorkomen
3. Groot: kan dagelijks voorkomen

Impact: effect als het risico waarheid wordt, de nadelige gevolgen.

1. Klein: verstoring niet-primaire proces, alleen intern merkbaar
2. Middel: verstoring primair proces, extern merkbaar, snel opgelost
3. Groot: verstoring primair proces, reputatieschade, langdurig

Risico	Kans	Impact	Maatregelen
Niet vergrendelen van de werkplek	Groot	Groot –	- Automatisch vergrendelen van applicaties/netwerk na bepaalde tijd.(hier zijn kosten aan verbonden, heb ik herman over gemaild) - Gebruikers bewust maken van de risico's.
Achterlaten/verlies/diefstal digitale media: - USB-sticks - Externe harde schijven - Mobiele telefoons - Laptops - Tablets	Middel	Groot –	- Verbieden van het gebruik van USB-sticks en externe harde schijven. - Goede vergrendeling van privé-apparaten ter bescherming van applicaties t.b.v. schoolwerk. - Privé-apparaten hebben een eigen inlog voor privacygevoelige of schoolinformatie, waardoor andere gebruikers (gezinsleden) niet bij deze gegevens kunnen.
Printopdrachten worden direct geprint	Groot	Groot –	- Beveiligd printen, waarbij iedere gebruiker moet inloggen om printopdrachten uit te printen.(zou ook een hoop papier schelen, ik ga navragen bij qlict of dit kan?) - Consumentenprinters mogen niet meer in het netwerk, vanwege de onmogelijkheden van het beheer.

Diefstal hardware	Middel	Groot ???	- Goede inbraakbeveiliging - Hardware in beheeromgeving, zodat deze op afstand te wissen zijn. - BIOS-vergrendeling
Applicaties: - Office 365/G-Suite/Apple/MDM - Lokale kopie/synchronisatie schijven - Basispoort/Software - Leeromgevingen gekoppeld aan netwerkbeheer	Middel	Groot +/-	- Automatisch inloggen in applicaties mag alleen ingeschakeld worden als het apparaat vergrendeld wordt met een sterk persoonlijk wachtwoord. - Wachtwoorden zijn niet zichtbaar op papier bij de werkplek. - Wachtwoorden die bewaard worden op iedere papieren vorm worden vernietigd als deze niet meer gebruikt worden. Ze mogen niet bij het oud papier belanden. - Het is niet toegestaan om dezelfde wachtwoorden voor hoog privacygevoelige inlog te hebben zoals mail en leerlingadministratie- en volgsystemen. - Softwareleveranciers moeten deelnemen aan het privacyconvenant en bereid zijn een bewerkersovereenkomst te tekenen, anders kan bij deze leverancier geen software(licentie) worden afgenomen na 1 augustus 2018.
Papieren dossiers / Adreslijsten - Leerlinggegevens - Financiële zaken - Personeelsgegevens	 - + +	??	- Het is niet toegestaan om zonder toestemming van ouders en medewerkers adreslijsten te verspreiden. - Papieren dossiers zijn opgeborgen in afgesloten kasten en/of ruimtes. - Papieren dossiers mogen nooit bij het oud papier, maar dienen vernietigd te worden.
Ongewenst delen van content sociale media: - Ouderportalen - Facebookpagina school	Middel + / - +/-		- Scholen hebben een overzicht per groep waaruit blijkt of ouders bezwaar hebben gemaakt tegen het publiceren van beeldmateriaal op de website, sociale media of een ander online portaal. - Scholen wijzen ouders elk jaar actief op de mogelijkheid om dit

			bezwaar te herzien of alsnog bezwaar te maken. - Scholen moeten hierbij specificeren voor welke onderdelen de media wordt gebruikt. Ouders moeten per medium aangeven of zij hiervoor toestemming geven. - Ouders hebben altijd het recht om hun toestemming in te trekken of een beeld als ongewenst te bepalen. - Bovenschools mogen alleen foto's gebruikt worden waarvan de ouders toestemming hebben gegeven voor het gebruik van deze foto's. - Ouders die geen respons geven, hebben geen akkoord gegeven. Dit betekent dat beeldmateriaal niet gebruikt mag worden.
Aanval: - DDos - Hack - Virus	Middel	Groot –	- De netwerkbeheerder zorgt voor een gedegen beveiliging van het netwerk. - Meerdere keren per jaar wordt er een mail verstuurd om personeel te waarschuwen voor deze aanvallen en hoe te handelen mocht dit toch gebeuren. - Scholen waarschuwen de netwerkbeheerder indien zij het gevoel hebben dat zij een virus hebben geopend op hun pc. - Naschoolse opvang en leerkrachten houden beter zicht op leerling die spellen spelen of wij verbieden computer gebruik?
Storing van: - Internetverbinding - Applicaties - Netwerkbeheer	Klein	Groot +/1	- Internetproviders versturen een mailing om locaties op de hoogte te brengen van werkzaamheden. - Het moet duidelijk zijn wie de contactpersonen van de provider zijn mocht de internetverbinding uitvallen.
Wachtwoorden - Om in te loggen op het netwerk - Om in te loggen in software - De pincode van het alarmsysteem - Codes van kluisjes/kluizen en kluisdeuren	Groot	Groot +	- Fysieke uitingen waarop wachtwoorden of pincodes zichtbaar zijn mogen in het schoolgebouw alleen opgeborgen worden in af te sluiten kasten. - Een wachtwoord bestaat tenminste uit 8 tekens, waarvan minimaal 1 hoofdletter, 1 kleine letter en 1 cijfer.