Bijlage 12

Procedure autorisatie en controle toegangsrechten

1. Doel

Vastleggen van de werkwijze en verantwoordelijkheden ten aanzien van de controle van toegangsrechten binnen de organisatie. Dit betreft toegang tot gebouw (sleutels, medewerkerspasjes), toegang tot intranet en toegang tot ICT-systemen.

Vul in welke pasjes en codes in de organisatie worden gebruikt:
……

2. Doelgroep

Alle medewerkers in de organisatie.

3. Afkortingen

indien van toepassing:

4. Voorbeeld: toewijzing toegangsrechten en controle hierop

Personeel krijgt, afhankelijk van de functie en locatie, sleutels van het pand of opbergkasten, een toegangspasje, een inlogcode voor het alarm, toegangsrechten voor het archiveringssysteem op intranet en toegang tot de gebruikte ICT-systemen.

Bij nieuwe medewerkers wordt gewerkt met een lijst aan de hand waarvan vastgesteld wordt welke rechten iemand moet krijgen tot al deze zaken.

Bij uitdiensttreding van medewerkers wordt aan de hand van het ‘uit dienst formulier’ gecheckt of alle rechten ook weer worden ingetrokken. Ook bij het wijzigen van functie worden de rechten herzien. Dit gebeurt in samenspraak tussen de leidinggevende en de P&O-adviseur.

Periodiek worden er controles gehouden op de toegangsrechten.
De wijze waarop die controle gebeurt, verschilt per toegangsrecht.

4.1 Toegang tot de gebouwen: sleutels, pasjes en codes

Voor elke locatie dient bekend te zijn welke personen toegang hebben tot het pand en met welke toegangscode.

Indien ex-medewerkers door middel van oude inlogcodes en/of sleutels zich toegang verschaffen tot het gebouw, computers en bestanden, dan is dit een beveiligingsincident. Dit dient gemeld te worden aan de locatiemanager, directeur en kwaliteitsfunctionaris. Voor deze overtreding kan aangifte gedaan worden.

4.2 Toegang tot archivering

Medewerkers met management-, staf- en administratieve taken ontvangen een code/nummer waarmee zij toegang krijgen tot delen van de archiveringsschijf. Vooraf wordt bepaald waar men in mag. Maak hiervan een overzicht dat door de leidinggevende wordt geaccordeerd.

Jaarlijks wordt het overzicht van de toegekende rechten gecontroleerd door de ICT-adviseur op juistheid. Afwijkingen worden beschouwd als beveiligingsincident en gemeld aan de kwaliteitsfunctionaris.

Bij nieuwe medewerkers wordt de juiste toekenning van de toegangsrechten op de eerste werkdag gecontroleerd door de direct leidinggevende.

4.3 Toegang tot het patiëntregistratiesysteem

Alle medewerkers in het zorgproces hebben via de UZI-pas toegang tot het patiëntregistratiesysteem.
Daarnaast heeft een aantal medewerkers beperkte rechten, zoals het secretariaat en de financiële administratie.

Het aanvragen, uitreiken en intrekken van UZI-passen en mandatering is vastgelegd in een procedure: zie bijlage UZI-passen.
Bij medewerkers die uit dienst treden is dit geregeld via het ‘uit dienst formulier'.

Voor huisartsen, waarnemers en AIOS: zodra een huisarts zijn/haar BIG-registratie of huisartsaantekening verliest, wordt de organisatie hierover door het UZI-register geïnformeerd. Deze berichten komen binnen bij het secretariaat, waar de aanvragen en intrekkingen van de UZI-passen worden geregeld. Het secretariaat meldt dit bij de directie.

5. Autorisatie

5.1 Autorisatietabel (functies kunnen in personen soms overlappen)

Functie	Sleutel	Toegangspasje	Inlogcode alarm	UZI pas	Toegang patiëntregistratie systeem	Archivering
Directie	x	x				x
Bestuur						
MT-leden	x	x				x
ICT adviseur	x	x			x	x
FA medewerkers	x	x		x	x	x
Secretariaatsmedew.	x	x		x	x	x
Locatiemanagers	x	x				x
Huisartsen				x	x	
Waarnemers				x	x	
AIOS				x	x	

6. Aparte systemen

6.1 Voicerecorder

Leg vast wie bevoegd is tot het beluisteren en kopiëren van bandopnamen. Leg vast wie toegang heeft tot het systeem, zodat bij wijzigen van functie of uitdiensttreding, de codes kunnen worden gewijzigd.

6.2 Personeelssysteem

Leg vast wie in dit systeem kunnen (indien voorhanden) en regel met aparte inlog dat de leidinggevenden alleen in de dossiers kunnen van de eigen medewerkers.

6.3 Relatiebeheersysteem (RBS)

Leg vast welke data uit het relatiebeheersysteem (huisartsen, medewerkers, externe relaties) openbaar mogen zijn voor de kantoormedewerkers, en welke vertrouwelijk zijn en dus beperkt toegankelijk moeten zijn.