Responsible Disclosure richtlijnen

RTV Oost vindt veiligheid van haar systemen erg belangrijk. Ondanks de zorg voor de beveiliging van de systemen en gegevens kan het voorkomen dat er een zwakke plek is. Indien u een kwetsbaarheid heeft gevonden in één van de ICT-systemen van RTV Oost (zoals www.rtvoost.nl of de RTV Oost App), hoort RTV Oost dit graag van u. Op deze manier kan de omroep zo snel mogelijk de benodigde maatregelen nemen om dit te verhelpen.

RTV Oost hanteert voor deze meldingen de *Responsible Disclosure* principes. Dat betekent dat u verantwoordelijk met de kwetsbaarheid om zult gaan (zoals hierboven beschreven) en de zwakke plek eerst zult melden aan RTV Oost, voordat u het aan de buitenwereld kenbaar maakt. Op deze manier kan RTV Oost eerst maatregelen nemen.

Wij vragen u:

- uw bevindingen te mailen naar privacy@rtvoost.nl;
- voldoende informatie te geven om het probleem te reproduceren, zodat RTV Oost zo snel mogelijk kan oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn;
- de melding zo snel mogelijk na de ontdekking van de kwetsbaarheid doen;
- schriftelijk te bevestigen dat u conform deze *'Responsible Disclosure'* heeft gehandeld en zult blijven handelen;
- de informatie over het beveiligingsprobleem niet met anderen te delen;
- verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem door geen handelingen te verrichten die verder gaan dan noodzakelijk om het beveiligingsprobleem aan te tonen;
- juiste contactgegevens achter te laten, zodat RTV Oost met u in contact kan komen om samen te werken aan een veilig resultaat. Indien u hiervoor kiest, laat dan minimaal uw naam, e-mailadres en/of telefoonnummer achter. Anoniem melden of melden onder een pseudoniem is mogelijk.

Vermijd de volgende handelingen:

- het plaatsen van malware;
- het kopiëren, wijzigen of verwijderen van gegevens in een systeem;
- het aanbrengen van veranderingen in het systeem;
- het herhaaldelijk toegang tot het systeem verkrijgen of de toegang delen met anderen;
- het gebruik maken van geautomatiseerde scantools;
- het gebruik maken van het zogeheten 'bruteforcen' van toegang tot systemen;
- het gebruik maken denial-of-service of social engineering;
- indien u bij de melding van een door u geconstateerde kwetsbaarheid in een ICT-systeem van RTV Oost aan de bovenstaande voorwaarden voldoet, zal RTV Oost geen juridische consequenties verbinden aan deze melding.

RTV Oost belooft u:

- indien de contactgegevens bekend zijn: te pogen binnen een werkdag een ontvangstbevestiging te sturen en binnen vijf werkdagen te reageren op uw melding. De reactie bevat een beoordeling van de melding en eventueel een verwachte einddatum voor een oplossing. Daarnaast houdt RTV Oost de melder op de hoogte van de voortgang van het oplossen van het probleem;
- het door u geconstateerde beveiligingsprobleem in een systeem zo snel mogelijk op te lossen;
- een melding vertrouwelijk behandelen en deelt persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is. RTV Oost kan, als u dat wilt, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.

Bovenstaand Responsible Disclosure beleid is gebaseerd op het beleid wat er geldt bij het Nationaal Cyber Security Centrum (NCSC), NOS en de Rijksoverheid.