

Bijlage CSR 1 Omgaan met vertrouwelijke informatie en documenten

CSR 1.1 Doelstelling

Medewerkers van Rijkswaterstaat en haar Opdrachtnemers moeten op de juiste wijze omgaan met vertrouwelijke informatie (documenten en gegevens). Dit is mede van groot belang voor de beveiliging van de ICT infrastructuur en de primaire processen van Rijkswaterstaat tegen cybercriminaliteit. Beveiliging van de informatievoorziening en bedienketens in het primair proces, hangt direct samen met de beveiliging van de documentatie betreffende de ICT-infrastructuur. De vertrouwelijkheid van informatie wordt uitgedrukt in een classificatie. De classificatie geeft de aard van de documentatie weer en helpt de gebruiker bij het bepalen hoe een document verwerkt dient te worden.

Rijkswaterstaat houdt de volgende rubricering of informatieclassificatie aan:

- a. Departementaal Vertrouwelijk;
- b. RWS Bedrijfsvertrouwelijk;
- c. RWS Bedrijfsinformatie.

Departementaal Vertrouwelijk

Deze informatie dient strikt vertrouwelijk te worden behandeld en mag uitsluitend op basis van need-to-know worden verstrekt. Informatie met deze classificatie mag niet worden uitgewisseld met Opdrachtnemers en valt derhalve buiten de scope van dit document.

RWS Bedrijfsvertrouwelijk

Deze informatie is uitsluitend toegankelijk voor diegenen die de informatie nodig hebben om hun werkzaamheden uit te kunnen voeren en wordt op basis van need-to-know verstrekt.

RWS Bedrijfsinformatie

Deze informatie is voor iedereen vrij toegankelijk.

CSR 1.2 Best practice

CSR 1.2.1 Uitwisselen van informatie

In de overeenkomst tussen Rijkswaterstaat en een Opdrachtnemer zijn eisen opgenomen voor geheimhouding en het vertrouwelijk omgaan met documenten.

Voorbeelden van RWS bedrijfsvertrouwelijke informatie (gerelateerd aan cybersecurity) zijn:

- a. Ontwerpdocumenten, constructietekeningen en -berekeningen;
- b. Bediening en beheer handleidingen, veiligheidsinstructies en documentatie;
- c. Configuratie-documentatie van ICT en ICS/SCADA-systemen;
- d. Datanetwerkschema's en IP adressen;
- e. Informatie over de ligging van kabels en leidingen;
- f. Informatie over accounts en wachtwoorden.

Uitwisseling van informatie kan op meerdere manieren plaatsvinden. Voor elke wijze van uitwisseling zijn specifieke voorwaarden en regels van kracht:

Informatie uitwisseling via email

- a. Informatie met de classificatie RWS Bedrijfsvertrouwelijk mag onversleuteld via email worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer.
- b. Informatie met de classificatie TLP AMBER mag onversleuteld via email worden uitgewisseld tussen Rijkswaterstaat en BAW partners.

Informatie uitwisseling via bestand-uitwisselingsservices

- a. Informatie met de classificatie RWS Bedrijfsvertrouwelijk via Wettransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer, waarbij bestanden worden versleuteld met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de

wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

- b. Informatie met de classificatie TLP AMBER via Wettransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en BAW partners, waarbij bestanden worden versleuteld met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

Informatie uitwisseling via servers van opdrachtnemer of opdrachtgever

Informatie met de classificatie RWS Bedrijfsvertrouwelijk of TLP AMBER mag onversleuteld via servers van opdrachtgever, opdrachtnemer of BAW partner worden uitgewisseld, mits er een voldoende authenticatie van de gebruiker en zijn bevoegdheden plaatsvindt.

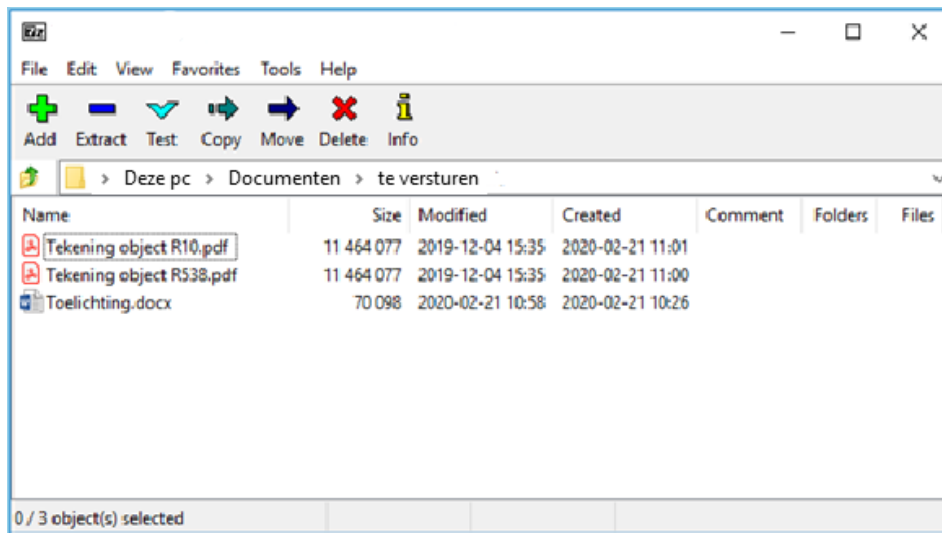
CSR 1.2.2 Versleutelen van gegevens

Wanneer versleuteling van informatie nodig is, dient dit te gebeuren met ten minste AES 256 encryptie en een sterk wachtwoord dat voldoet aan de vereisten voor wachtwoorden. Voor versleuteling maakt RWS gebruik van 7-Zip. Dit is een eenvoudig te gebruiken computerprogramma, waarmee bestanden versleuteld ingepakt kunnen worden.

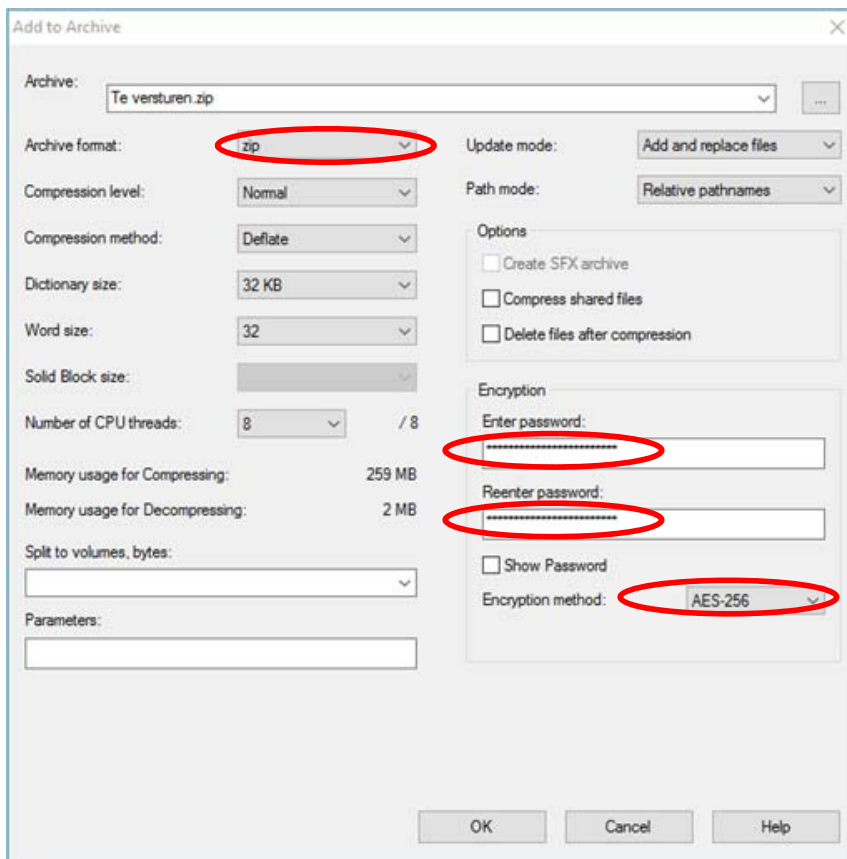
7-Zip is standaard aanwezig op de RWS werkplek en is tevens gratis voor (thuis)gebruik (zie www.7-zip.org). Bij gebruik van AES-256 versleuteling en sterke wachtwoorden (zie hiervoor de wachtwoordrichtlijn) biedt 7-Zip een veilige manier voor gegevensversleuteling.

Documenten versleutelen met 7-Zip

- a. Start 7-Zip via de Start toets links onderin Windows.
- b. Ga naar de folder waar de te versleutelen bestanden staan.



- c. Selecteer de bestanden en klik op de Add button (het groene + symbol).



- d. Selecteer:
 - i. Archive format: zip
 - ii. Encryption method: AES-256
- e. Kies een wachtwoord dat voldoet aan de wachtwoordrichtlijn en voer dit in.
- f. Klik op de OK button en sluit 7-Zip af.
- g. Het versleutelde bestand is klaar om te versturen.

Documenten ontsleutelen met 7-Zip

- a. Open het bestand in 7-zip.
- b. Selecteer de Extract button (het blauwe  symbool).
- c. Selecteer de folder waar het bestand uitgepakt dient te worden.
- d. Voer het wachtwoord in en klik de OK button.

CSR 1.2.3 Overdracht en vernietiging van vertrouwelijke data bij einde contract

Bij het aflopen en beëindiging van een contract draagt de Opdrachtnemer alle voor het onderhoud (en onderhoudshistorie) relevante objectinformatie -met de classificatie Bedrijfsvertrouwelijk- gestructureerd over aan Rijkswaterstaat.

Daarna vernietigt Opdrachtnemer de overgebleven Bedrijfsvertrouwelijke informatie en verwijdert deze alle Bedrijfsvertrouwelijke informatie van de eigen systemen.