WebProof er sikkerhedscertificeret

Hvor sikker er din korrektur af dokumenter?

Vi lever i en usikker verden. Og når vi siger verden, mener vi både den virkelige verden og cyberspace. Men først og fremmest mener vi den digitale verden, hvor vi udfører de fleste af vores forretningsaktiviteter. Ikke mindst når det drejer sig om korrektur af dokumenter. Dokumentkorrektur gør dig ekstremt sårbar.

Hvorfor?

Fordi du sandsynligvis benytter e-mail, som er et både gammeldags og forældet værktøj. Og fra et sikkerhedsmæssigt perspektiv er det et mareridt. Alle dine filer er spredt, mens du forsøger at holde styr på tusindvis af e-mails som en del af korrekturprocessen. Kan du sikre, at alle disse e-mails har de nødvendige sikkerhedsindstillinger? Kan du sikre, at der ikke benyttes private e-mailadresser? Selvfølgelig kan du ikke det. Og det er præcist det, som hackere og cyberkriminelle ved. Findes der en løsning?

Dokumentkorrektur i et trygt og sikkert miljø

WebProof er en onlineplatform til dokumentsamarbejde og -korrektur, hvor sikkerheden har højeste prioritet. WebProof efterlader ikke plads til fejltagelser eller kompromisser, når det drejer sig om kundernes sikkerhed. Det er også værd at bemærke, at WebProof er en af de få SaaS-virksomheder (Software-as-a-Service), som har opnået den anerkendte ISO 27001-sikkerhedscertificering. ISO 27001-certificeringen dækker både WebProofs software og cloud-hosting-løsning.


QSL
Certificate of Registration
WebProof a/s
ISO Quality Services Limited
ISO 27001 : 2013
QSL
AUDIT SERVICES

ISO 27001 sikkerhedscertifikat Webproofs

Her har du det

ISO 27001-sikkerhedscertificering er din garanti for, at WebProof giver dig den højeste sikkerhed. Og går du og overvejer, om WebProof selv er en sikker virksomhed, er der også styr på den side af sagen. WebProof er en økonomisk stabil virksomhed med AAA-kreditvurdering. Færre end to procent af alle virksomheder har opnået denne vurdering. Så det er ikke helt uvæsentligt!

Hvad betyder det så for dig og din dokumentkorrektur? Først og fremmest er ISO 27001-sikkerhedscertificeringen din garanti for sikkerhed i topklassen. Derudover kan du trygt bruge korrekturtjenesterne og -værktøjerne uden at skulle bekymre dig om, at de en dag måske ikke længere er tilgængelige som følge af økonomiske vanskeligheder eller økonomisk ustabilitet.

Sikkerhedsstandarder i topklassen til vigtige kunder

Hvis du vil vide mere om ISO 27001-sikkerhedscertificering, er det blot at google det eller kontakte vores supportteam. Det kan give dig en idé om, hvor vanskeligt og komplekst det er at opnå denne certificering. Du vil nok også sætte pris på, at du ikke skal bekymre dig om sikkerhedsrisici og kompromittering af følsomme virksomhedsoplysninger, når dine dokumenter skal læses af andre.

Hvad er Adobes syn på SaaS-sikkerhed?

94 % af alle virksomheder er i dag helt afhængige af SaaS. Derudover viser undersøgelser foretaget af den canadiske forskningsgruppe Info-Tech Research Group, at langt de fleste it-chefer har større tillid til SaaS-sikkerhed end til deres egne sikkerhedsløsninger og -ressourcer. WebProof er Adobe-partner og følger derfor alle sikkerhedstendenser tæt og validerer pålideligheden for SaaS-sikkerhed på daglig basis. Her er rapporten om SaaS-sikkerhed fra Info-Tech Research Group, så du selv kan se, hvad vi taler om. Adobe opfordrer på det kraftigste sine partnere til at opnå sikkerhedscertificeringer og anvende de højeste SaaS-sikkerhedsstandarder.

WebProof viderefører sin politik om kun at anvende branchens mest prestigefyldte og pålidelige certificeringer. Vi sørger for, at din dokumentkorrektur til enhver tid er effektiv, økonomisk og ikke mindst sikker!

Hvad er ISO 27001 ISMS-certificering?

Et ISMS-system (Information Security Management System) er en systematisk og proaktiv tilgang til effektiv administration af sikkerhedsrisici i relation til en virksomheds fortrolige oplysninger.
Systemet fremmer effektiv administration af følsomme virksomhedsoplysninger og identificerer sikkerhedsrisici for at sikre, at oplysningerne beskyttes korrekt.
Det omfatter sikkerhed for lokaler, medarbejdere, processer og it-systemer, så du kan være sikker på, at WebProof ikke går på kompromis med beskyttelse af sine data.

Du kan downloade WebProofs ISO 27001-certifikat her: WebProofs ISO 27001-certifikat

Standarderne i ISO/IEC 27000-serien hjælper virksomheder med at beskytte informationsaktiver. Standarderne hjælper virksomheden med at administrere sikkerhed for aktiver, herunder økonomiske oplysninger, immateriel ejendom, medarbejderdata eller oplysninger, som er blevet overdraget til virksomheden af tredjepart. ISO/IEC 27001, som er seriens bedst kendte standard, stiller krav om et ledelsessystem for informationssikkerhed (ISMS).

Hvad er et ISMS?

Et ISMS-system er en systematisk tilgang til at administrere og beskytte følsomme virksomhedsoplysninger. Det omfatter en risikoadministrationsproces for medarbejdere, processer og it-systemer. Det er udviklet til at hjælpe små, mellemstore og store virksomheder i alle brancher med at beskytte sikkerheden for informationsaktiver.
Du kan finde de gratis tilgængelige afsnit i ISO/IEC 27001:2013 på ISO's Online Browsing Platform. Du kan købe standarden i ISO Store.

Ligesom andre ISO-standarder for ledelsessystemer er certificering i henhold til ISO/IEC 27001 ikke obligatorisk, men et valg. Nogle virksomheder vælger at implementere standarden for at drage fordel af de best practice-fremgangsmåder, den indeholder, mens andre vælger at blive certificerede for at forsikre kunderne om, at standardens anbefalinger er blevet fulgt. ISO udfører ikke selv certificering.

Læs mere om certificering i henhold til ISO's standarder for ledelsessystemer.

WebProof bruger Amazon Cloud pga. sikkerheden

WebProof valgte for flere år siden at flytte mere end 100 millioner filer fra sin egen serverpark til Amazon Cloud, ikke for at opnå økonomiske besparelser, men derimod for at opnå større sikkerhed for alle aspekter, herunder belastningsjustering og clustering.

WebProof bruger Amazon Web Services (AWS) som cloud-center, fordi det er verdens sikreste hosting-partner. Hosting-centeret er baseret i Irland, så det opfylder også EU's databeskyttelseskrav. AWS er endvidere certificeret i henhold til ISO 27001-standarden for informationssikkerhed.


Certificate

Certificate number: 2013-009
Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

headquartered in Seattle, Washington, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: November 11, 2013
Re-issue date of certificate: December 4, 2015
Expiration date of certificate: November 12, 2016

EY CertifyPoint will, according to the certification agreement dated October 23, 2014), perform surveillance audits and acknowledges the certificate until the expiration date of the certificate.

*This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in Statement of Applicability, approved on October 22, 2015.

Drs. R. Toppen RA
Director EY CertifyPoint

Beskrivelse af Amazon 27001-compliance

ISO 27001 er en sikkerhedsstandard med best practice-fremgangsmåder for administration af sikkerhed og omfattende sikkerhedskontroller. Certificeringen er baseret på udvikling og implementering af et strengt sikkerhedsprogram, herunder et ISMS-system (Information Security Management System), som definerer AWS' holistiske og omfattende tilgang til at administrere sikkerhed. Den anerkendte internationale sikkerhedsstandard kræver, at enheder skal opfylde følgende:

- Systematisk evaluere alle sikkerhedsrisici for data under hensyntagen til virksomhedens trusler og svaghedspunkter
- Designe og implementere en komplet pakke med informationssikkerhedskontroller og andre former for risikostyring for at håndtere sikkerhedsrisici for virksomheden og dens arkitektur
- Implementere en overordnet administrationsproces for at sikre, at informationssikkerhedskontrollerne hele tiden opfylder vores behov for informationssikkerhed.

AWS' implementering og overholdelse af ISO 27001, 27017 og 27018 demonstrerer virksomhedens store indsats for at beskytte informationer på alle niveauer. AWS' overholdelse af ISO 27001-standarden evalueres af en uafhængig tredjeparts-auditor. Overholdelse af disse internationalt anerkendte standarder og regelsæt garanterer, at AWS-sikkerhedsprogrammet er komplet og i overensstemmelse med brancheførende best practice-fremgangsmåder.

AWS' ISO 27001-certificering kan downloades her.

WebProof-sikkerhedselementer og -nøgleord til beskyttelse af dine data.

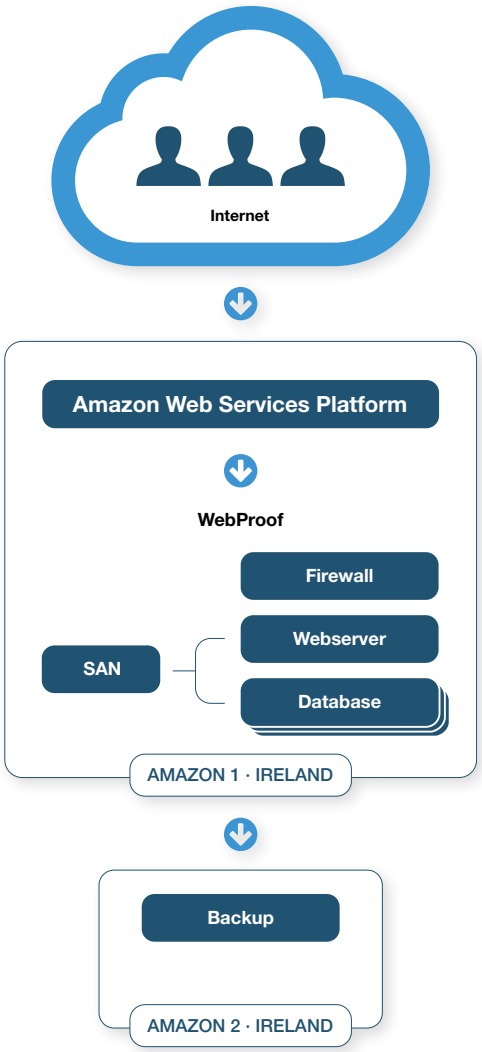
Sikkerhed kan i store træk inddeles i sikkerhed for cloud-hosting-center, for programmer, for brugere, for udvikling/fejlfinding og produktion, for udviklingsmiljø og for WebProofs organisation. Alle områder er lige vigtige, og intet område er stærkere end det svageste led. ISO 27001 er derfor en vigtig standard, fordi den sikrer, at ISMS-systemet holdes opdateret. Alle i organisationen er involveret i ISO 27001 ISMS-standarden.

Både WebProof-softwaren og vores organisation anvender LEAN-principper, hvor ISO 27001 er en naturlig følge af to af reglerne – systematisk opfølgning, forbedring, opfølgning, forbedring osv.

Vi vil ikke beskrive alle de detaljer, der indgår i beskyttelsen af dine data, men her er svar på nogle af de spørgsmål, vi oftest bliver stillet (se næste side).

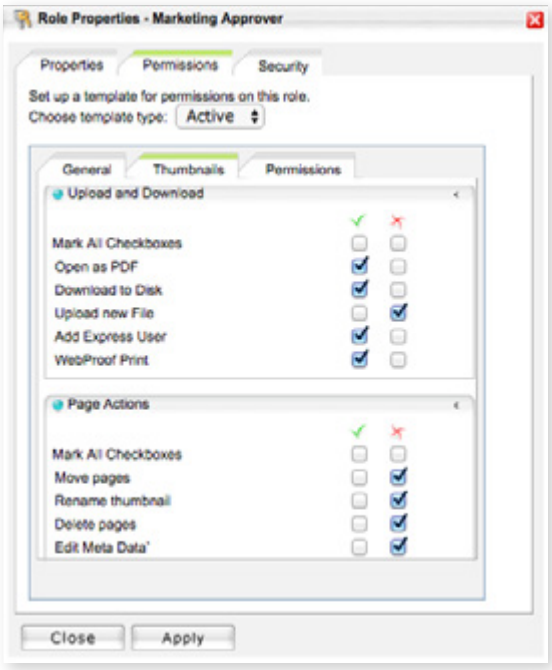
Ofte stillede spørgsmål

- *Cloud-hosting – vi bruger Amazon Web Services, som har verdens bedste sikkerhed. AWS overholder EU's databeskyttelsesprotokoller og er både ISO 27001- og ISO 9001-certificeret. Datacenteret opfylder alle de hyppigst anvendte globale standarder og sikkerhedsprotokoller. Vores datacenter hostes af Amazon i Irland. AWS har flere cloud-placeringer og teleudbydere, så du aldrig risikerer hastighedsbegrænsninger eller mulige afbrydelser af internetforbindelsen. Du kan finde flere oplysninger om Amazon nedenfor og på Amazon Web Service-webstedet.*
- *Der er en hurtig og nem plan for genoprettelse efter nedbrud. Den er baseret på vores clustering-opsætning med fysisk adskilte servere, der fungerer som øjeblikkelig backup.*



- *Serverparken har beskyttet sikkerhed, herunder spejling, clustering og firewall-sikkerhed.*
- *Ingen servere deler den samme masteradgangskode.*
- *Der er en fuldt redundant opsætning uden et enkelt fejlpunkt for hardware eller netværksopsætning.*
- *Kundedata og -databaser holdes adskilt på serverniveau. Så der ikke er nogen risiko for forveksling, heller ikke i tilfælde af en menneskelig fejl.*
- *WebProof understøtter bl.a. HTTS, FTP-S og TLS.*
- *WebProof kører en fuld indtrængningsscanning mindst en gang i kvartalet. Scanningen udføres af tredjepart.*
- *WebProof er 100 % webbaseret. Du skal blot have en browser. Der kræves hverken Java, plugins, tilføjelsesprogrammer eller Flash!*

- *WebProof har en avanceret løsning til administration af tilladelser og rettigheder, som betyder, at kun den korrekte bruger kan få adgang til den korrekte version.*

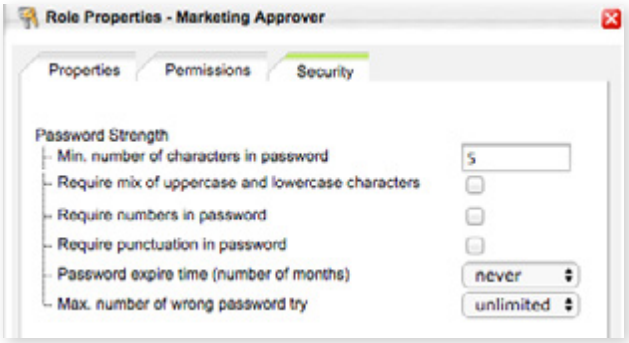


- *Kunden kan låse for synlig adgang til bestemte sider i et projekt. Funktionen bruges typisk til at låse sider i årsrapporter for børsnoterede selskaber eller sider med foreløbige regnskabstal.*

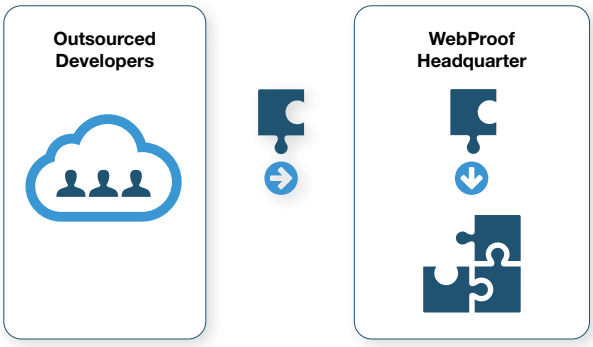
- *Beskyttelse mod ormevirus i PDF-dokumenter (brugeren åbner altid kun en JPG og skal ikke downloade den tilhørende PDF).*
- *Det er muligt at gendanne data for den seneste uge. Hvis du utilsigtet sletter et projekt, kan vi gendanne det for dig med det samme.*
- *WebProof gør det muligt at gemme historik og data i arkiver, så længe du ønsker.*
- *Den garanterede oppetid er 99,9 % over en periode på tre måneder, hvilket svarer til mindre end fem minutters nedetid i døgnet. Skulle vi imod forventningen ikke være i stand til at overholde denne garanti, kompenserer vi dig for den ekstra nedetid.*
- *Planlagt vedligeholdelse af software og hardware finder altid sted i weekenden på et tidspunkt, hvor statistikken viser, at trafikken er mindst, så afbrydelsen for kunderne er minimal.*
- *Bag vores firewalls er systemerne beskyttet med blandt andet oversættelse af netværksadresser og IP-adresser.*

Ofte stillede spørgsmål

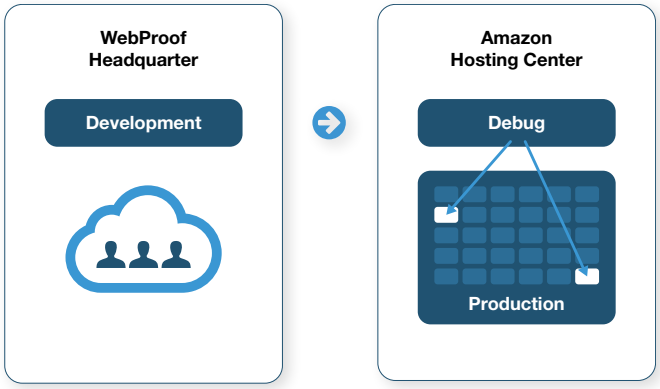
- *Adgangskoden krypteres og hash-beskyttes, så den ikke kan ses af nogen, heller ikke WebProof.*
- *Du kan anmode om et 2048-bit SSL-certifikat*
- *Sikkerhedsopsætningen for brugeradgangskoder kan tilpasses af administratoren for kundens WebProof-løsning, men skal som minimum omfatte et brugernavn og en adgangskode med fem tegn, der gemmes som et beskyttet MD5-hash, så den ikke kan dekrypteres af hverken WebProof eller andre. Brugeren kan kun logge på, hvis det korrekte brugernavn og adgangskoden kendes.*



- *Alle brugerdata, f.eks. IP-adresser, logføres.*
- *Vi kan på anmodning udvide adgangskodeløsningen med en SMS-kode, som skal bruges til godkendelse, når brugere logger på, og der avendes en særlig statuskode. Dette er i overensstemmelse med del 11 i den amerikanske CFR-lovgivning, som minder om ISO 27001-sikkerhedscertificeringen.*
- *Alle kundedata i WebProof-oversigter kan eksporteres som XML-data. Der kan også oprettes ledelsesrapporter for alle aktiviteter enten direkte eller til sorteringsformål.*
- *Kunderne kan få IP-begrænsninger med deres løsning, hvilket betyder, at kun brugere fra visse IP-adresser kan logge på.*
- *Sikkerheden for vores system er allerede blevet godkendt af it-afdelingerne hos vores store kunder, f.eks. LEGO, COOP, ICA og andre store anerkendte brands.*
- *WebProof har et stort netværk af udviklere i forskellige lande, så vi som nogle af de få har adgang til kompetente udviklingsressourcer over hele verden. For os er det viden og ikke den fysiske placering, som er vigtig. Eksterne udviklere har kun begrænset adgang til hovedkontorets udviklingsservere. De har aldrig adgang til kundedata.*



- *WebProofs egne udviklere sidder i vores hovedkontor. De konfigurerer alle funktionerne i WebProof og sikrer, at de lever op til WebProofs standarder. WebProof ejer og kontrollerer altid al kildekode til alt, hvad vi udvikler. Kun tre personer i WebProofs hovedkontor har adgang til kundernes produktionssystemer, og først når du har givet dem tilladelse til det. Ingen som helst kan få logisk adgang til kundedata, medmindre kunden oplyser brugernavnet og adgangskoden.*
  Adgangskoder gemmes aldrig som almindelig tekst, men udelukkende i et beskyttet hash-format, som ikke kan dekrypteres.
- *WebProof-software udvikles på en anden fysisk adresse end hosting-centeret. De to steder er fuldstændig uafhængige af hinanden.*



- *Når udviklingsstedet er klar med en opdatering, opdateres fejlfindingsmiljøet på hosting-stedet. Fejlfindingsmiljøet er konfigureret på samme måde som produktionsstedet, men er adskilt fra produktionsstedet, hvis der skulle opstå problemer.*
- *Når opdateringen er blevet testet og godkendt i fejlfindingsmiljøet, overføres den til et eller flere af produktionsstedets aktive systemer.*
- *Hvert af produktionsstedets aktive systemer har sin egen private beholder til data, database og web. Det betyder, at det er muligt at teste en opdatering på få udvalgte aktive systemer, uden at de øvrige aktive systemer påvirkes. Når opdateringen har kørt stabilt i en periode, anvendes den på alle de aktive systemer. Hvor længe opdateringen kører på en isoleret del af produktionssystemet, afhænger af opdateringens kompleksitet.*
- *Det tager kun få timer at teste en mindre fejlrettelse, mens det kan tage flere uger at teste store opdateringer. Øjeblikkelig tilbagerulning er også muligt, hvis opdateringen giver uønskede resultater.*
- *Alle WebProofs medarbejdere har underskrevet en fortrolighedsaftale, som stiller strenge krav til identifikation og bekræftelse.*
- *Vi bruger godkendelse med flere faktorer (MFA), så vi kun kan få adgang til systemet med et brugernavn og en stærk adgangskode samt en personlig engangskode, som ændres en gang i minuttet.*