IBM MobileFirst Protect (SaaS)

Vilkår for brug består af disse IBM Vilkår for brug – SaaS-specifikke produktvilkår (kaldet SaaS-specifikke produktvilkår) og dokumentet IBM Vilkår for brug – Standardvilkår (kaldet Standardvilkår), som er tilgængeligt på adressen http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

I tilfælde af en uoverensstemmelse har de SaaS-specifikke produktvilkår forrang for Standardvilkårene. Ved at bestille, tilgå eller benytte IBM SaaS-produktet accepterer Kunden disse Vilkår for brug.

Disse Vilkår for brug er reguleret af IBM International Passport Advantage-Aftalen, IBM International Passport Advantage Express-Aftalen eller IBM International Aftale om Udvalgte IBM SaaS-produkter (hver især kaldet Aftalen), som sammen med Vilkår for brug udgør den fuldstændige aftale.

1. IBM SaaS

De SaaS-specifikke produktvilkår dækker følgende IBM SaaS-produkt:

- IBM MobileFirst Protect – Devices (SaaS)
- IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Applications (SaaS)
- IBM MobileFirst Protect – Applications (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Application Security (SaaS)
- IBM MobileFirst Protect – Application Security (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway for Apps (SaaS)
- IBM MobileFirst Protect – Gateway for Apps (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Content (SaaS)
- IBM MobileFirst Protect – Content (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Document Sync (SaaS)
- IBM MobileFirst Protect – Document Sync (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Document Editor (SaaS)
- IBM MobileFirst Protect – Document Editor (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway for Documents (SaaS)
- IBM MobileFirst Protect – Gateway for Documents (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Email Management (SaaS)
- IBM MobileFirst Protect – Email Management (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Browser (SaaS)
- IBM MobileFirst Protect – Browser (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway for Browser (SaaS)
- IBM MobileFirst Protect – Gateway for Browser (SaaS) Step up for existing customers
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Expenses (SaaS)
- IBM MobileFirst Protect – Expenses (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Management Suite (SaaS)
- IBM MobileFirst Protect – Management Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Productivity Suite (SaaS)
- IBM MobileFirst Protect – Productivity Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Secure Mail (SaaS)

- IBM MobileFirst Protect – Secure Mail (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Threat Management (SaaS)
- IBM MobileFirst Protect – Content Service (SaaS)
- IBM MobileFirst Protect – Content Service Storage (SaaS)
- IBM MobileFirst Protect – Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect – Laptop (SaaS)
- IBM MobileFirst Protect – Laptop Location (SaaS)
- IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)
- IBM MaaS360 Professional Bundle Prime (SaaS)
- IBM MaaS360 Educational Bundle Prime (SaaS)
- IBM MaaS360 Advanced Laptop Management Prime (SaaS)

2. Måletyper for betaling

IBM SaaS-produktet sælges og betales på basis af en af følgende målinger, som angivet i Transaktionsdokumentet:

a. **Autoriseret Bruger (Authorized User)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Kunden skal anskaffe separate, dedikerede brugsrettigheder til hver entydige Autoriserede Bruger, som – uanset måde – får adgang til IBM SaaS-produktet direkte eller indirekte, f.eks. via et multiplex-program, en enhed eller en applikationsserver, uanset metode. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder til at kunne dække det antal Autoriserede Brugere, som får adgang til IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

b. **Gigabyte (Gigabyte)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. En Gigabyte defineres som 2 i 30. byte data (1.073.741.824 byte). Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder til at kunne dække det samlede antal Gigabyte, som håndteres af IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

c. **Administreret Client-enhed (Managed Client Device)** – er en måleenhed, som IBM SaaS kan anskaffes på basis af. En Client-enhed er en enkelt brugers IT-enhed, en sensor til et specielt formål eller en telemetrienhed, som anmoder om gennemførelse af eller modtager – med henblik på udførelse – et sæt kommandoer, procedurer eller applikationer fra, eller leverer data til, et andet computersystem, der typisk kaldes en server, eller som administreres af serveren. Flere Client-enheder kan være fælles om adgangen til en server. En Client-enhed kan have en vis databehandlingskapacitet eller kan programmeres, så en bruger kan arbejde på den. Kunden skal anskaffe brugsrettigheder til Administrerede Client-enheder for hver Client-enhed, som administreres af IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

d. **Client-enhed (Client Device)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. En Client-enhed er en enkelt brugers IT-enhed, en sensor til et specielt formål eller en telemetrienhed, som anmoder om gennemførelse af eller modtager – med henblik på udførelse – et sæt kommandoer, procedurer eller applikationer fra, eller leverer data til, et andet computersystem, der typisk kaldes en server, eller som administreres af serveren. Flere Client-enheder kan være fælles om adgangen til en server. En Client-enhed kan have en vis databehandlingskapacitet eller kan programmeres, så en bruger kan arbejde på den. Kunden skal anskaffe brugsrettigheder til hver Client-enhed, som kører, leverer data til, bruger serviceydelser leveret af eller på anden måde får adgang til IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

3. Pris og fakturering

Det beløb, der skal betales for IBM SaaS-produktet, er angivet i et Transaktionsdokument.

3.1 Betaling for del af måned

Betaling for en del af en måned, som angivet i Transaktionsdokumentet, kan opgøres forholdsvist.

3.2 Betaling for merforbrug

Hvis Kundens faktiske brug af IBM SaaS-produktet i måleperioden overstiger den brugsret, som er angivet i beviset for brugsret, bliver Kunden faktureret for merforbruget, som angivet i Transaktionsdokumentet.

4. Fornyelse af IBM SaaS-abonnementsperioden

Kundens bevis for brugsret vil angive, om IBM SaaS-produktet fornys ved Abonnementsperiodens udløb. Beviset angiver en af følgende muligheder:

4.1 Automatisk fornyelse

Hvis Kundens bevis for brugsret angiver, at fornyelsen sker automatisk, kan Kunden opsige den IBM SaaS-abonnementsperiode, der udløber, via skriftlig anmodning til Kundens IBM-salgskonsulent eller IBM Business Partner mindst 90 dage inden udløbsdatoen, som er angivet i beviset for brugsret. Hvis IBM eller Kundens IBM Business Partner ikke modtager en sådan anmodning inden udløbsdatoen, bliver Abonnementsperioden automatisk fornyet med ét år eller med samme varighed som den oprindelige Abonnementsperiode, der er angivet i beviset for brugsret.

Antallet af fornyede brugsrettigheder svarer til det største antal af følgende: Antallet i den oprindelige ordre eller den månedligt rapporterede brug inden genereringen af fornyelsesfakturaen. Dette antal gælder, medmindre IBM modtager en meddelelse, som angiver et andet antal.

Antallet af fornyede brugsrettigheder for produkter af typen Step-up svarer til antallet i den oprindelige ordre.

4.2 Løbende fakturering

Hvis der i beviset for brugsret står, at fornyelse sker løbende, har Kunden fortsat adgang til IBM SaaS-produktet og vil løbende blive faktureret for brug af IBM SaaS-produktet. Hvis Kunden ikke længere vil bruge IBM SaaS-produktet og ønsker at standse den løbende fakturering, skal Kunden med 90 dages skriftligt varsel til IBM eller Kundens IBM Business Partner anmode om, at Kundens IBM SaaS-produkt bliver annulleret. Når Kundens adgang annulleres, bliver Kunden faktureret for eventuelle udestående betalinger for adgang til og med den måned, hvor annulleringen trådte i kraft.

4.3 Fornyelse påkrævet

Hvis der i beviset for brugsret står, at Kundens brug af IBM SaaS-produktet ophører på fornyelsestidspunktet, ophører IBM SaaS-produktet ved udgangen af Abonnementsperioden, og Kundens adgang til IBM SaaS-produktet fjernes. Hvis Kunden vil bruge IBM SaaS-produktet efter udløbsdatoen, skal Kunden afgive en ordre hos IBM's salgskonsulent eller en IBM Business Partner om køb af en ny Abonnementsperiode.

5. Teknisk support

I abonnementsperioden er der inkluderet teknisk support af IBM SaaS i form af support på andet niveau til en kundes driftsteam, ikke slutbrugersupport.

Support leveres ad flere kanaler, 24 i døgnet, alle ugens 7 dage. Der er oplysninger om support af IBM SaaS-løsningen på produktportalen.

Mål for forventet reaktionstid:

Problemklassificering	Definition af problemklassificering	Indledende Målsætning for reaktionstid	Dækning – reaktionstid
1	**Funktion/serviceydelse med central indvirkning på forretningen er nede:** En central forretningsfunktion er ude af drift, eller der er fejl på en central grænseflade. Det gælder sædvanligvis et produktionsmiljø og angiver manglende adgang til serviceydelser, hvilket resulterer i en væsentlig påvirkning af driften. Tilstanden kræver en øjeblikkelig løsning.	30 minutter	24 x 7
2	**Stor indvirkning på forretningen:** Der er en alvorlig brugsbegrænsning i en forretningsfunktion i serviceydelsen, eller der er risiko for, at tidsfrister ikke overholdes.	1 arbejdstime	24 x 7
3	**Mellemstor indvirkning på forretningen:** Angiver, at serviceydelsen eller funktioner kan benyttes, og at der ingen alvorlig påvirkning er af driften.	2 arbejdstimer	24 x 7
4	**Lille indvirkning på forretningen:** En forespørgsel eller ikke-teknisk anmodning.	3 arbejdstimer	24 x 7

6. Tillægsvilkår for IBM SaaS-produktet

6.1 Begrænsninger i forbindelse med Step up

For IBM SaaS-produkter af typen "Step up for existing Customers" (kaldet Step up SaaS) gælder det, at Kunden tidligere eller samtidig skal have anskaffet en relevant licensrettighed til det IBM-program, som indgår i navnet på Step up SaaS-produktet. For eksempel skal Kunder, som køber IBM MobileFirst Protect – Devices (SaaS) – Step up for existing customers, have licensrettigheder til IBM-programmet IBM MobileFirst Protect. Kundens rettigheder til Step up SaaS kan ikke overstige de rettigheder, Kunden har til det tilknyttede IBM-program.

Hvis Kunden anskaffer Step up SaaS, må Kunden ikke bruge de samme licensrettigheder til et tilknyttet IBM-program i sit lokale, installerede miljø og sammen med Step up SaaS-rettighederne. Hvis Kunden for eksempel har brugsrettigheder til 250 Administrerede Client-enheder til det tilhørende IBM-program og vælger at købe 100 brugsrettigheder til Administrerede Client-enheder til Step up SaaS, kan Kunden administrere 100 Administrerede Client-enheder til Step Up SaaS fra IBM SaaS-miljøet og 150 Administrerede Client-enheder fra den software, der er installeret hos Kunden.

Kunden erklærer, at Kunden har anskaffet (1) de relevante licensrettigheder og (2) relevant Abonnement og Support til det eller de tilhørende IBM-programmer. I Abonnementsperioden på Step up SaaS-produktet skal Kunden opretholde aktuel Abonnement og Support til de IBM-programrettigheder, som anvendes sammen med Step up SaaS-rettighederne. Hvis Kundens licens til brug af det eller de tilhørende IBM-programmer eller Kundens Abonnement og Support til det eller de tilhørende IBM-programmer ophører, ophører Kundens ret til at benytte Step up SaaS-produktet også.

6.2 Cookies

Kunden accepterer, at IBM må bruge cookies og sporingsteknologi til at indsamle personoplysninger i forbindelse med brugsstatistik og oplysninger, som kan hjælpe med at forbedre brugernes oplevelse og/eller til at skræddersy interaktion med brugerne. Indsamlingen sker i henhold til http://www-01.ibm.com/software/info/product-privacy/index.html.

6.3 Overførsel på tværs af grænser

Hvis Kunden stiller Personoplysninger til rådighed for IBM SaaS-produkter i EU's medlemsstater, Island, Liechtenstein, Norge eller Schweiz, Tyrkiet eller et andet europæisk land, som har vedtaget lokal databeskyttelseslovgivning, accepterer Kunden, at IBM må behandle Indhold, herunder eventuelle Personoplysninger, i henhold til relevante love og krav, på tværs af landegrænser til databehandlere og underdatabehandlere i følgende lande uden for Det Europæiske Økonomiske Samarbejdsområde og lande, der af Europa-Kommissionen anses for at have et tilstrækkeligt sikkerhedsniveau:

Navn på databehandler/underdatabehandler	Rolle (Databehandler eller Underdatabehandler)	Sted
IBM Corporation	Underdatabehandler	1 New Orchard Rd. Armonk, NY 10504, USA I
IBM India Private Limited	Underdatabehandler	Nr. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 Indien

Kunden accepterer, at IBM med et varsel kan ændre landelisten, hvis IBM med rimelighed beslutter, det er nødvendigt for leveringen af IBM SaaS-produktet.

6.4 Databeskyttelse i EU

Hvis Kunden gør Personoplysninger tilgængelige for IBM SaaS-produkter i EU's medlemsstater, Island, Liechtenstein, Norge eller Schweiz, Tyrkiet eller et andet europæisk land, som har vedtaget lokal databeskyttelseslovgivning, eller hvis Kunden har autoriserede brugere eller enheder i disse lande, udpeger Kunden som fuldt dataansvarlig IBM som databehandler (som disse udtryk er defineret som henholdsvis "registeransvarlig" og "registerfører" i EU-direktiv 95/46/EF) til at behandle Personoplysninger. IBM behandler kun sådanne Personoplysninger i det omfang, det er nødvendigt for at gøre IBM SaaS-produktet tilgængeligt i overensstemmelse med IBM's offentliggjorte beskrivelser af IBM SaaS-produktet, og Kunden bekræfter, at enhver sådan behandling er i overensstemmelse med Kundens anvisninger.

6.5 Overholdelse af Safe Harbor-principperne

IBM SaaS-produkterne er inkluderet i Fiberlink Communications Corporations (IBM-datterselskab) US-EU Safe Harbor-certificering. Både IBM og Fiberlink overholder principperne i Safe Harbor-ordningen, som er aftalt mellem EU og USA, som angivet af det amerikanske handelsministerium, vedrørende indsamling, brug og opbevaring af oplysninger, der indsamles fra EU. Der er flere oplysninger om Safe Harbor-ordningen og om Fiberlinks certificering på http://www.export.gov/safeharbor/.

I de tilfælde, hvor principperne i Safe Harbor-ordningen, som er aftalt mellem USA og EU, ikke gælder en overførsel af Personoplysninger fra EØS (Europæiske Økonomiske Samarbejdsområde), kan parterne eller deres relevante associerede eller koncernforbundne virksomheder indgå separate aftaler ved brug af EU's uændrede standardaftaler i deres aktuelle roller i henhold til EU-beslutning 2010/87/EU, hvor de valgfri betingelser er fjernet. Parterne skal behandle enhver uenighed eller forpligtelse, som opstår i forbindelse med disse aftaler – også selvom aftalen er indgået af en associeret eller koncernforbunden virksomhed – som om uenigheden eller forpligtelsen er opstået mellem parterne under vilkårene i denne Aftale.

6.6 Lokaliteter med afledte fordele (Derived Benefit)

Hvor det er relevant, baseres skatter og afgifter på den eller de lokationer, Kunden identificerer som værende den eller de lokationer, der modtager fordelen ved IBM SaaS-produktet. IBM inkluderer skatter og afgifter på basis af den forretningsadresse, Kunden anfører som primær fordelslokalitet ved bestilling af et IBM SaaS-produkt, medmindre Kunden informerer IBM om andet. Det er Kundens ansvar at sørge for, at oplysningerne er opdateret og at informere IBM om eventuelle ændringer.

6.7 Normative data

Medmindre andet er angivet kan IBM – udelukkende til brug i normativ forskning, demonstration, rapportering og normative analyser – opbevare og bruge data i samlet, anonymt format (dvs. så Kunden eller Kundens autoriserede brugere ikke kan identificeres som kilde til dataene, og så personligt identificérbare oplysninger om Kunden eller Kundens autoriserede brugere er fjernet), som afspejler Kundens autoriserede brugeres individuelle oplevelser med IBM SaaS.

6.8 Retmæssig brug og samtykke

6.8.1 Bemyndigelse til at indsamle og behandle data

IBM SaaS-produktet er designet til at levere, administrere, sikre, overvåge og kontrollere mobile enheder. IBM SaaS-produktet indsamler oplysninger fra brugere og enheder, som Kunden har autoriseret til at interagere med det IBM SaaS-produkt, som Kunden abonnerer på. IBM SaaS-produktet indsamler oplysninger, der alene eller samlet kan anses for Personoplysninger i nogle jurisdiktioner. Indsamlede data kan omfatte navn på autoriseret bruger, telefonnummer, registreret e-mailadresse og enhedsplacering, bruger-id og historik for sikker browsing, oplysninger om hardware, software og indstillinger for slutbrugerenhed og informationer, som er genereret af enheden. Kunden giver IBM tilladelse til at indsamle, behandle og anvende disse informationer i overensstemmelse med vilkårene i disse Vilkår for brug.

6.8.2 Informeret samtykke fra registrerede personer

Brugen af IBM SaaS-produktet kan være underlagt forskellige love eller regler. IBM SaaS-produktet må kun anvendes til lovlige formål og på lovlig vis. Kunden erklærer sig indforstået med at anvende IBM SaaS-produktet i henhold til relevante love, regler og politikker og påtager sig ethvert ansvar for at overholde disse.

Kunden bekræfter, at Kunden har indhentet eller vil indhente alle fuldt informerede samtykker, tilladelser eller licenser, der er nødvendige for lovlig brug af IBM SaaS-produktet, og som tillader IBM som Kundens databehandler at indsamle og behandle oplysninger via IBM SaaS. Kunden bemyndiger hermed IBM til at indhente de fuldt informerede samtykker, der er nødvendige for at muliggøre lovlig brug af IBM SaaS-produktet og for at indsamle og behandle oplysninger som beskrevet i slutbrugerlicensaftalen, der kan ses på http://www.ibm.com/software/sla/sladb.nsf/.

6.9 Dataopbevaring

IBM sletter alle indsamlede oplysninger, som kan inkludere Personoplysninger, når disse Vilkår for brug ophører, medmindre oplysningerne skal opbevares til de formål, der er angivet ovenfor eller i relevant lovgivning, relevante regler eller bestemmelser. I så fald opbevarer IBM de indsamlede oplysninger, så længe formålet, relevant lovgivning, relevante regler eller bestemmelser kræver det.

Bilag A

MobileFirst Protect er en brugervenlig cloud-platform, som har alle de funktioner, der er væsentlige for en komplet styring af mobile enheder i dag, herunder iPhones, iPads, Androids, Kindle Fire-enheder, Windows Phones og BlackBerry-smartphones. Nedenfor følger en kort beskrivelse af IBM SaaS-produktet:

1. IBM MobileFirst Protect – Devices (SaaS)

De centrale MDM-funktioner (mobility device management) inkluderer tilmelding og konfiguration af enheder, administration af sikkerhedspolitik og enhedshandlinger, f.eks. send meddelelse, find, lås og slet. De avancerede MDM-funktioner inkluderer automatiseret regeloverholdelse, BOYD-fortrolighedsindstillinger (bring your own device) og Mobility Intelligence-dashboards og -rapportering.

2. IBM MobileFirst Protect – Applications (SaaS)

MobileFirst Protect Applications giver mulighed for at tilføje applikationer og distribuere dem til understøttede enheder, der administreres via MobileFirst Protect. Det inkluderer MobileFirst Protect App Catalog, der er en applikation på enheden, som brugeren kan anvende til at få vist, installere og få meddelelse om opdaterede og administrerede applikationer.

3. IBM MobileFirst Protect – Application Security (SaaS)

MobileFirst Protect Application Security tilbyder ekstra databeskyttelse til virksomhedsapplikationer, der benytter WorkPlace SDK i forbindelse med udvikling, eller til iOS-apps, som nemt kan uploade applikationen (.ipa), tilknytte den til implementeringsprofiler og automatisk integrere et underskriftscertifikat. Mobile Application Security integrerer appen med Secure Productivity Suite. Det muliggør et enkelt logon, intranetadgang via Mobile Enterprise Gateway og håndhævelse af indstillinger for datasikkerhed.

4. IBM MobileFirst Protect – Gateway for Apps (SaaS)

MobileFirst Protect Gateway for Apps tilbyder brugere uden for virksomhedsnetværket en sikker, problemfri adgang til interne applikationsressourcer, uden at brugerne skal have en VPN-forbindelse på fuldt enhedsniveau.

5. IBM MobileFirst Protect – Content (SaaS)

MobileFirst Protect Content giver administratoren mulighed for at tilføje dokumenter og distribuere dem til de understøttede enheder, som administreres af IBM MobileFirst Protect Devices. Produktet inkluderer IBM MobileFirst Protect Doc Catalogue, et kodeordsbeskyttet opbevaringssted på enheden, som tilbyder brugerne adgang til, fremvisning og deling af dokumenter på en nem måde. Det inkluderer problemfri adgang til distribueret indhold og opbevaringssteder, f.eks. SharePoint, Box og Google Drive. MobileFirst Protect Mobile Enterprise Gateway giver adgang til private SharePoint- og Windows-fildelinger. Dokumenter, der administreres via MobileFirst Protect, kan versionskontrolleres, revideres og sikres via DLP-regelindstillinger (data loss prevention), f.eks. at de kræver validering, at der er begrænsede muligheder for at klippe og klistre, og at de kan blokeres, så de ikke kan åbnes i eller deles med andre applikationer.

6. IBM MobileFirst Protect – Document Sync (SaaS)

MobileFirst Protect Document Sync giver brugerne mulighed for nemt og sikkert at synkronisere brugerindhold på tværs af administrerede, mobile enheder. Administratorer kan sikre, at regler, f.eks. en begrænsning i klippe-klistre-funktionen og blokering af indhold, så det ikke kan åbnes eller deles i andre apps, er på plads for brugerindhold på tværs af enheder. Indholdet opbevares sikkert – både i skyen og på enheden – og adgang kan kun ske via MobileFirst Protect Doc Catalogue.

7. IBM MobileFirst Protect – Document Editor (SaaS)

MobileFirst Protect Document Editor er en kraftfuld kontorserie, som giver brugerne mulighed for at arbejde med forretningsdokumenter, mens brugerne er på farten. Med MobileFirst Protect Secure Editor kan brugerne:

- Oprette og redigere DOC-, PPT- og XLS-filer.
- Benytte præsentationstilstand til dias
- Nemt arbejde med vedhæftede filer i e-mail og med andre filer i MobileFirst Protect til iOS.

8. IBM MobileFirst Protect – Gateway for Documents (SaaS)

Med MobileFirst Protect Gateway for Documents kan virksomheder bruge MobileFirst Protect Content til også at tilbyde enheder uden for virksomhedens netværk sikker, problemfri adgang til interne Connections-websteder, SharePoint-websteder, Windows File Shares og andre fillagre, uden at der kræves en komplet VPN-forbindelse. Brug af MobileFirst Protect Gateway for Documents kræver køb af MobileFirst Protect Content. Understøtter iOS 5.0 og Android 4.0 eller nyere.

9. IBM MobileFirst Protect – Email Management (SaaS)

MobileFirst Protect Email Management inkluderer centrale funktioner, som understøtter Microsoft Exchange ActiveSync og Lotus Traveler.

- Exchange ActiveSync: Tilbyder support til mobile enheder, som opretter forbindelse til Microsoft Exchange via ActiveSync-protokollen. Funktionerne inkluderer vigtige funktioner til administration af mobile enheder, f.eks. konfiguration og oprettelse af enheder, gennemtvingelse af ActiveSync-politikker (adgangskode, blokering eller adgangstilladelse til e-mail) og handlinger i forbindelse med enheder, f.eks. lås og tømning af enheder for data, og detaljerede rapporter om enhedsattributter.
- Lotus Traveler: Support til mobile enheder, som opretter forbindelse til IBM Lotus Notes via Lotus Traveler-protokollen. Funktionerne inkluderer mulighed for at konfigurere enheder, blokere eller tillade enheder, gennemtvinge en politik for adgangskoder, slette alle data fra enheder og udvikle detaljerede rapporter om enhedsattributter.

10. IBM MobileFirst Protect – Browser (SaaS)

MobileFirst Protect Browser er en webbrowser med alle funktioner. Den sørger for sikker adgang til virksomheders intranetwebsteder og gennemtvinger overholdelse af indholdspolitik ved at definere regler for webstedsfiltrering og sikkerhed. Det sikrer, at brugere kun får adgang til godkendt webindhold baseret på en række indholdskategorier, f.eks. sociale netværk eller malwarewebsteder. Browseren giver også mulighed for at deaktivere indbyggede browsere eller tredjepartsbrowsere, enten via en applikationspolitik eller sortlistning, i kombination med MobileFirst Protect Devices. Det giver mulighed for hvidlistningsundtagelser til websteder og begrænsning af cookies; funktioner til kopiering, indsætning og udskrivning og aktivering af Kiosk-tilstand.

11. IBM MobileFirst Protect – Gateway for Browser (SaaS)

MobileFirst Protect Gateway for Browser giver understøttede enheder mulighed for adgang til godkendte interne websteder uden krav om en VPN-forbindelse på fuldt enhedsniveau.

12. IBM MobileFirst Protect for Blackberry (SaaS)

Tilbyder support til BES-tilsluttede (BlackBerry Enterprise Server) mobilenheder via BlackBerry API'er. Funktionerne omfatter eksterne handlinger, f.eks. afsendelse af besked, nulstilling af kodeord, tilknytning af BES-politik og tømning af enheden for data samt detaljeret rapportering om enhedsattributter. Installation af MobileFirst Protect Cloud Extender er påkrævet. Er kun tilgængelig for enheder, som vises eller administreres med MobileFirst Protect via BES 5.0.

13. IBM MobileFirst Protect – Expenses (SaaS)

MobileFirst Protect Expenses giver administratoren mulighed for at oprette politikker for brug af data og tilknytte dem til understøttede enheder, der administreres af MobileFirst Protect. Politikkerne kan tilknyttes på enhedsniveau, gruppeniveau eller globalt niveau. Derudover kan administratoren konfigurere tærskelværdier for advarsler og beskedudveksling i forbindelse med af brug af data, både i netværk og via roaming.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Produktpakke, inklusive MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content og MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Produktpakke, inklusive MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content og MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

MobileFirst Protect Secure Mail tilbyder en separat og sikker kontorapplikation, som giver brugerne adgang til og mulighed for at administrere e-mail, kalender og kontaktpersoner. Derudover giver applikationen mulighed for at styre e-mail og vedhæftede filer, så datalækage kan forhindres. Det kan ske ved at begrænse muligheden for at sende eller flytte indhold til andre applikationer, via krav til validering, begrænsning af klik-kopiér-indsæt-funktion samt låsning af vedhæftede filer i e-mail, så de kun kan vises.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

Med MobileFirst Protect Gateway Suite kan understøttede apps på iOS og Android kommunikere tilbage til virksomhedens interne netværk på en sikker og problemfri måde.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Produktpakke, inklusive MobileFirst Protect Content, MobileFirst Protect Document Editor og MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

MobileFirst Protect Threat Management tilbyder udvidet sikkerhed til mobilenheder via påvisning af malware og udvidet påvisning af jailbreaking eller rooting. Med MobileFirst Protect Threat Management kan Kunden angive og administrere politik for overholdelse af lovgivning og regler i forbindelse med påvist malware og andre sikkerhedssårbarheder.

20. IBM MobileFirst Protect – Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) gør det muligt for brugerne at uploade applikationspakker og dokumenter til MobileFirst Protect Content Distribution-systemet.

Kunder, som har MobileFirst Protect Content Service, skal også købe mindst én brugsrettighed til både MobileFirst Protect Content Service Storage (SaaS) og MobileFirst Protect Content Service Bandwidth (SaaS).

21. IBM MobileFirst Protect – Content Service Storage (SaaS)

MobileFirst Protect Content Service Storage (SaaS) giver brugerne mulighed for at købe en samlet mængde datastorage, som kan benyttes sammen med MobileFirst Protect Content Service (SaaS).

22. IBM MobileFirst Protect – Content Service Bandwidth (SaaS)

MobileFirst Protect Content Service Bandwidth (SaaS) giver brugerne mulighed for at købe en samlet mængde båndbredde, som kan benyttes sammen med MobileFirst Protect Content Service (SaaS).

23. IBM MobileFirst Protect – Professional (SaaS)

Giver mindre og mellemstore virksomheder mulighed for hurtigt og nemt via ekstern adgang at konfigurere smartphones og tablets, at gennemtvinge en sikkerhedspolitik, overføre apps og dokumenter og beskytte data på virksomhedsejede og på private enheder. Kunden kan hurtigt, nemt og til en fornuftig pris få adgang til de helt rigtige funktioner til administration af mobilt udstyr.

24. IBM MobileFirst Protect – Laptop (SaaS)

Giver Kunden mulighed for at tilmelde sig, konfigurere, administrere, sikre og rapportere på OS X- og Windows PC-baserede enheder sammen med smartphones og tablets. Virksomheder kan opretholde ensartede sikkerhedspolitikker og -profiler på tværs af såvel virksomheds- som medarbejderejede enheder inden for den samme MobileFirst Protect-administrationskonsol.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) til Windows-baserede computere tilbyder trådløs tilmelding og rapportering om enheder på basis af hardware-, styresystems- og softwareoplysninger. Modulet til

rapportering om slutpunktssikkerhed tilbyder interaktiv rapportering om og dataanalyse til kundeleverede applikationer, for eksempel antivirus, sikkerhedskopiering/retablering, datakryptering og personlig firewall samt manglende programrettelser til styresystem.Databeskyttelsesmodulet tilbyder interaktiv rapportering om og analyse til sikkerhedsydelser, herunder datakryptering, forebyggelse af datatab, sikkerhedskopiering/retablering og andre integrerede applikationer. Understøtter Windows XP SP3, Windows Vista, Windows 7, Windows 8+ og Windows 8+ Pro (inklusive 32-bit og 64-bit, hvor der er relevant).

Enhedshandlinger omfatter:

- Sende besked til enheden
- Låse enheden
- Finde enheden (kræver MobileFirst Protect Laptop Location)
- Standse/starte/genstarte serviceydelser
- Lukke ned/genstarte
- Tømme harddisken for data
- Konfigurere indstillinger for programrettelser
- Distribuere software

24.2 Mac OS X

MobileFirst Protect – Laptop (SaaS) til Mac OS X tilbyder trådløs tilmelding og rapportering om enheder på basis af hardware-, styresystems- og softwareoplysninger. Modulet til rapportering om slutpunktssikkerhed tilbyder interaktiv rapportering om og dataanalyse til kundeleverede applikationer, for eksempel antivirus, sikkerhedskopiering/retablering, datakryptering og personlig firewall samt manglende programrettelser til styresystem.Databeskyttelsesmodulet tilbyder interaktiv rapportering om og analyse til sikkerhedsydelser, herunder datakryptering. Modulet til konfigurationsstyring tilbyder ekstern styring af en række enheder og brugerindstillinger, herunder kodeord, e-mail, VPN og WiFi. Understøtter Mac OS X version 10.7.3 eller nyere.

Enhedshandlinger omfatter:

- Låse enheden
- Tømme harddisken for data
- Ændre enhedspolitik

25. IBM MobileFirst Protect – Laptop Location (SaaS)

MobileFirst Protect Laptop Location (SaaS) har gjort det muligt at finde understøttede bærbare computere og tablets. MobileFirst Protect rapporterer om placeringen af koordinaterne for WiFi- eller IP-adressen og oversætter dataene til en nemt genkendelig adresse. Når en enhed er online, hentes oplysninger om dens aktuelle placering. MobileFirst Protect opbevarer rapporterede oplysninger om placering over tid, så placeringshistorikken kan gennemses. Kræver IBM MobileFirst Protect Laptop (SaaS) til Windows. Understøtter Windows XP SP3, Windows Vista, Windows 7, Windows 8+ og Windows 8+ Pro (inklusive 32-bit og 64-bit, hvor der er relevant).

26. IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)

Indeholder funktionerne i MobileFirst Protect – Laptop (SaaS) samt følgende ekstra funktioner:

- Mulighed for at uploade pakker til MobileFirst Protect Content Service-platformen (SaaS) og planlægge distribution af data til enheder, som administreres af MobileFirst Protect Laptop-serviceydelsen (SaaS) til Microsoft Windows. Kunden styrer alle aspekter af distributionen, herunder installationsvejledning og retning mod mål på enheds- eller gruppeniveau eller på globalt niveau. Kunden er ansvarlig for al pakning og for oprettelse af installationsfil. IBM tilbyder ikke at understøtte oprettelse af installationspakke.

27. IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)

Tilbyder virksomheder mulighed for at opretholde en ensartet sikkerhedspolitik og ensartede profiler på tværs af såvel virksomheds- som medarbejderejede enheder inden for samme administrationskonsol.

28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

De centrale MDM-funktioner (mobility device management) inkluderer tilmelding og konfiguration af enheder, administration af sikkerhedspolitik og enhedshandlinger, f.eks. send meddelelse, find, lås og slet. De avancerede MDM-funktioner inkluderer automatiseret regeloverholdelse, BOYD-fortrolighedsindstillinger (bring your own device) og Mobility Intelligence-dashboards og -rapportering.

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Giver mulighed for at få adgang til e-mail, opbevare, distribuere og administrere applikationer og give adgang til intranetwebsteder på en sikker måde ved brug af Secure Browser.

30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Giver mulighed for via fjernadgang at administrere og konfigurere smartphones og tablet-computere, gennemtvinge sikkerhedsregler, distribuere data og rapportere om WiFi-brug, hvilket kan bruges til at spore databrug og udgifter, samt for indholdslagring og -distribution til applikationer og dokumenter.

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Giver mindre og mellemstore virksomheder mulighed for via fjernadgang at konfigurere smartphones og tablets, at gennemtvinge en sikkerhedspolitik, overføre apps og dokumenter og beskytte data på virksomhedsejede og på private enheder.

32. IBM MaaS360 Educational Bundle Prime (SaaS)

Giver uddannelsesinstitutioner mulighed for via fjernadgang at administrere og konfigurere smartphones og tablet-computere, gennemtvinge sikkerhedsregler og distribuere data samt for indholdslagring og -distribution til applikationer samt for administration af applikationer.

33. IBM MaaS360 Advanced Laptop Management Prime (SaaS)

Giver virksomheder mulighed for at administrere, opdatere, placere og distribuere software til laptop-computere og på den måde pålægge ensartede sikkerhedsregler på tværs af alle laptop/desktop-computere, der rapporterer til MaaS360-administrationskonsollen.

Bilag B

IBM tilbyder følgende aftale om Servicemål (SLA) for tilgængelighed for IBM SaaS-produktet. Aftalen finder anvendelse, hvis den er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

Den version af denne SLA, som gælder på tidspunktet for abonnementets ikrafttrædelse eller fornyelse, er gældende for aftalen. Den enkelte Kunde er indforstået med, at SLA'en ikke udgør en garanti.

1. Definitioner

a. **Autoriseret Kontaktperson** – betyder den person, som Kunden over for IBM har udpeget som autoriseret til at fremsende krav i henhold til denne SLA.

b. **Begivenhed** – betyder en omstændighed eller en række omstændigheder, som samlet betyder, at et Servicemål ikke overholdes.

c. **Force Majeure** – betyder naturkatastrofer, terrorisme, faglige aktioner, brand, oversvømmelse, jordskælv, optøjer, krig, offentlig regulering, offentlige påbud eller restriktioner, virus, DOS-angreb (denial of service) og anden ondsindet adfærd, svigt i forbindelser til forsyningsværker og netværk eller enhver anden form for manglende IBM SaaS-tilgængelighed, som ligger uden for IBM's rimelige kontrol.

d. **Kontraheret Måned** – betyder hver hele måned i IBM SaaS-produktets løbetid, målt fra midnat den første dag i måneden til og med kl. 23.59 den sidste dag i måneden.

e. **Krav** – betyder et krav, som den Autoriserede Kontaktperson har sendt til IBM i henhold til vilkårene i denne SLA, og som indeholder en påstand om, at et Servicemål ikke er opfyldt i en måned, som er omfattet af aftalen (kontraheret måned).

f. **Krediteringsbeløb på grund af manglende tilgængelighed (Availability Credit)** – betyder det beløb, IBM tilbyder i forbindelse med et valideret krav. Availability Credit tilbydes i form af et krediteringsbeløb eller en rabat på en senere faktura for betaling af abonnement på IBM SaaS-produktet.

g. **Kunde**, **De** eller **du** – betyder en enhed, som abonnerer på IBM SaaS-produktet direkte hos IBM, og som ikke har misligholdt en væsentlig forpligtelse, herunder en betalingsforpligtelse, i henhold til Kundens aftale med IBM om IBM SaaS-produktet.

h. **Nedetid** – betyder Applikationsnedetid og/eller Nedetid for behandling af indgående data, som gælder for det tilhørende Servicemål, der vises i tabellen nedenfor. Nedetid omfatter ikke den tid, hvor IBM SaaS-produktet ikke er tilgængelig som følge af:

- Planlagt Systemnedetid.
- Force majeure.
- Problemer med kunde- eller tredjepartsapplikationer, -udstyr eller -data.
- Handlinger eller undladelser fra Kundens eller tredjeparts side, herunder det, at en person får adgang til IBM SaaS-produktet ved brug af Kundens kodeord eller udstyr.
- Manglende overholdelse af de krævede systemkonfigurationer og understøttede platforme, som giver adgang til IBM SaaS-produktet, eller
- IBM's overholdelse af de design, specifikationer eller instruktioner, som Kunden har givet, eller som tredjepart har givet på Kundens vegne.

i. **Planlagt Systemnedetid** – betyder planlagt afbrydelse af IBM SaaS-produktet med vedligeholdelsesformål for øje.

j. **Servicemål** – betyder den standard, der er angivet nedenfor, og som IBM bruger som mål for, om IBM leverer det Servicemål, IBM skal, i henhold til denne SLA.

2. Availability Credits

a. Før Kunden kan indsende et Krav, skal Kunden have oprettet en problemrapport (ticket) for hver Begivenhed hos den IBM-kundesupporthelpdesk, som tager sig af det relevante IBM SaaS-produkt. Det skal ske i henhold til IBM's procedurer for rapportering af problemer med problemklassificeringskode 1 (Severity 1). Kunden skal give alle nødvendige oplysninger om Begivenheden og i rimeligt omfang hjælpe IBM med fejlfinding og problemløsning i forbindelse med Begivenheden, som det kræves ved en problemrapportering med klassificeringskode 1. Sådanne rapporter skal være registreret inden for fireogtyve (24) timer, efter at Kunden første gang opdagede, at Begivenheden påvirkede Kundens brug af IBM SaaS-produktet.

b. Kundens Autoriserede Kontaktperson skal indsende Kravet om Availability Credit senest tre arbejdsdage efter udgangen af den Kontraherede Måned, som Kravet omfatter.

c. Kundens Autoriserede Kontaktperson skal give IBM alle relevante oplysninger, som vedrører Kravet, herunder f.eks. detaljerede beskrivelser af alle relevante Begivenheder og af det Servicemål, som Kunden hævder ikke er opfyldt.

d. IBM måler internt den samlede Nedetid for hver Kontraheret Måned, som gælder for det tilhørende Servicemål, der vises i tabellen nedenfor. Availability Credits baseres på varigheden af Nedetiden, målt fra det tidspunkt, som Kunden har rapporteret, at Kunden første gang blev påvirket af Nedetiden. Hvis Kunden rapporterer, at der er indtruffet en Begivenhed med Applikationsnedetid og en Begivenhed med Nedetid mht. Behandling af Indgående Data samtidigt, så behandler IBM de overlappende nedetidsperioder som en enkelt nedetidsperiode, og ikke som to separate nedetidsperioder. IBM anvender den højeste, relevante Availability Credit til hvert gyldigt Krav, baseret på det opnåede Servicemål i hver enkelt Kontraheret Måned, som vist i tabellen nedenfor. IBM er ikke ansvarlig for flere Availability Credit-beløb for samme Begivenhed(er) i samme Kontraherede Måned.

e. For så vidt angår pakkede Serviceydelser, det vil sige individuelle IBM SaaS-produkter, der pakkes og sælges sammen til én samlet pris, beregnes Availability Credit på basis af den samlede månedlige pris på de pakkede Serviceydelser og ikke på basis af det månedlige abonnementsgebyr for hvert enkelt IBM SaaS-produkt. Kunden kan kun indsende et Krav vedrørende ét individuelt IBM SaaS-produkt i en pakke i en Kontraheret Måned, og IBM hæfter ikke for Availability Credits for mere end ét IBM SaaS-produkt i en pakke i en Kontraheret Måned.

f. Hvis Kunden har købt IBM SaaS-produktet fra en godkendt IBM-forhandler i en videresalgstransaktion, hvor IBM har det primære ansvar for at opfylde forpligtelserne i forbindelse med IBM SaaS-produktet og SLA'en, baseres Availability Credit på den dengang gældende RSVP-pris (Relationship Suggested Value Price) for IBM SaaS-produktet for den Kontraherede Måned, som kravet omfatter, nedsat med 50 %.

g. Den samlede Availability Credit, som Kunden får tildelt for en Kontraheret Måned, kan under ingen omstændigheder overstige 10 % af en tolvtedel (1/12) af det beløb, Kunden betaler IBM årligt for IBM SaaS.

h. IBM foretager et rimeligt skøn ved validering af Krav, baseret på de oplysninger, der er tilgængelige i IBM's registreringer, og disse registreringer har forrang i tilfælde af en uoverensstemmelse med data i Kundens egne registreringer.

i. De Availability Credits, som Kunden får tilbudt i henhold til denne SLA, er Kundens eneste retsmiddel i forbindelse med et Krav.

3. Servicemål

IBM SaaS-tilgængelighed i en Kontraheret Måned

Opnået Servicemål (i en Kontraheret Måned)	**Availability Credit (% af den månedlige abonnementsbetaling for den Kontraherede Måned, som er genstand for Kravet)**
Under 99,8 %	2 %
Under 98,8 %	5 %
Under 95,0 %	10 %

Opnået Servicemål, udtrykt i procent, beregnes på denne måde: (a) det samlede antal minutter i en Kontraheret Måned minus (b) Nedetid i alt i minutter i en Kontraheret Måned divideret med (c) det samlede antal minutter i en Kontraheret Måned.

Eksempel: 50 minutters Nedetid i alt i en Kontraheret Måned

43.200 minutter i alt i en Kontraheret Måned på 30 dage - 50 minutters Nedetid = 43.150 minutter _____ 43.200 minutter i alt	= 2 % Availability Credit for et Opnået Servicemål på 99,8 % i den Kontraherede Måned

4. Undtagelser

Denne SLA gælder kun IBM-kunder. Denne SLA gælder ikke følgende:

- Beta- og prøveserviceydelser.
- Ikke-produktionsmiljøer, herunder for eksempel test, retablering efter katastrofe, kvalitetssikring eller udvikling.
- Krav fremsat af en IBM-Kundes brugere, gæster, deltagere og tilladte inviterede, som bruger IBM SaaS-produktet.
- Aktiveringssoftware