IT-Användarpolicy

2018-01-25

Rackfish AB

DOKUMENTNAMN:	IT-användarpolicy	SKAPAT DEN:	2009-09-14
TYP AV DOKUMENT:	Policy	SENAST ÄNDRAT DEN:	2018-01-25
FILNAMN:	IT-användarpolicy	VERSION:	2018 v1
DOKUMENTÄGARE:	Rackfish CTO		

IT-ANVÄNDARPOLICY

Denna IT-användarpolicy skapar en gemensam plattform för användandet av Rackfish IT-system. Den gäller alla, anställda såväl som konsulter och tillfälligt anställda m.fl. som ska använda Rackfish interna nät och system.

MÅL OCH SYFTE

Målet för Rackfish IT-användarpolicy är att genom tydliga instruktioner förenkla användandet av Rackfish interna nät och system i syfte att ge en säker IT-miljö där den efterfrågade informationen finns tillgänglig för rätt behörighet.

INFORMATION OCH ANSVAR

Det är upp till varje medarbetare att ansvara för att denna policy följs. Det är också varje medarbetares ansvar att anmäla brott eller föraning om brott mot denna policy.

Rackfish IT-användarpolicy kommer att ändras och det är upp till alla medarbetare att hålla sig uppdaterad om förändringar i policyn.

Vid brott mot denna policy har Rackfish rätt att vidta arbetsrättsliga åtgärder.

RESURSANVÄNDNING

IT ska godkänna all utrustning som ska anslutas till Rackfish interna nätverk.

Utrustning som tilldelats via IT är godkänd.

Gästdatorer får endast ansluta till Rackfish öppna Internetanslutningar, t.ex. WLAN PDI_Guest.

Inga resurser inom Rackfish IT-system får användas till att skicka, motta eller lagra information som är:

• diskriminerande eller som kan anses trakasserande

• nedvärderande mot en enskild person eller mot en grupp av individer

• relaterat till porr eller andra former av sexuell karaktär

• skadlig för annan person eller egendom

• ett brott mot svensk lag, t ex nedladdning av upphovsrättsskyddat material

• skadligt för eller missgynnar Rackfish intressen.

Rackfish förbehåller sig rätten att kontrollera användning av Rackfish mejl, interna system och Internet i syfte att säkerställa en säker IT-miljö där system och nätverk används i ett för Rackfish positivt syfte.

Rackfish anställda, samt övriga berörda parter, bör utgå från att information som skapas och distribueras med hjälp av Rackfish IT-system inte är privat.

MEJLANVÄNDNING

Rackfish mejl ska i huvudsak användas i arbetssyfte och registrering, såsom konton, i olika former för privat bruk får inte göras med Rackfish mejladresser.

Mejlen är en viktig informationskälla för företaget och inga mejl med affärsanknytning får raderas om det inte innan lagts in i godkänt dokumenthanteringssystem.

Detta kan röra t.ex. leveranser, inköp, bestridanden, offerter mm. IT kan arkivera alla mejl vid anställningens upphörande om skäl finns.

LÖSENORDSPOLICY

Lösenord till den enskilda datorn eller system är grunden för en säker IT-miljö. Alla ska vara medvetna om hur ett bra lösenord ska vara och tillämpa detta i sitt val av lösenord.

Lösenordet ska:

- vara minst 15 tecken långt
- innehålla stora och små bokstäver, siffror samt symbol (ex. #+&)
- inte innehålla användarnamnet, företagsnamnet, egennamn eller andra kända namn
- byts vid behov, t ex vid upptäckt virus, misstanke om att det kommit till någon annans kännedom etc.
- byts minst var tredje månad
- Lastpass används för att lagra gemensamma lösenord till system och webbtjänster.

En komplett guide och test för lösenord finns på

https://www.dinsakerhet.se/sakrare-hemma/teknik-och-it/losenord/

Tänk på att lösenordet är personligt. Lämna inte ut lösenordet till någon! Inte till chef, datoradministratör eller familjemedlem. Förvara eller skicka inte lösenord i klartext.

INSTANT MESSAGING (IM)

Företaget använder Slack för kommunikation internt men observera att det inte är tillåtet att nämna information som innehåller personuppgifter och annat känsligt data.

Andra produkter för chat & kollaboration kan användas om kund eller leverantör önskar använda den specifika produkten.

LAGRING AV ARBETE

För att information ska vara tillgänglig för organisationen och säkrad genom backup ska arbetsmaterial, dokument mm, lagras i Evernote, filservern eller i aktuellt system. Att spara på arbetsstationens/bärbara datorns hårddisk får endast ske i undantagsfall.

Backup av arbetsstation/bärbar dator sker till USB-disk med Time Machine eller annan godkänd mjukvara. Backuper skall vara krypterade

Rackfish lagringsmedia, hårddisk, filserver etc, får inte användas för lagring av personliga filer, mediafiler mm.

Känslig information får ej lämnas framme vid arbetsplats.

SÄKERHET VID NEDLADDNING AV FILER

- Ladda aldrig ner filer från okända eller osäkra siter
- Virusinfekterade datorer ska genast tas bort från nätverket, gäller även trådlös anslutning, och datorn måste installeras om från grunden.

DATORADMINISTRATION

Rackfish IT tilldelar rättigheter i nätverk och system baserat på arbetsuppgifter och godkännande från CEO. Då Rackfish är ett IT-bolag med hög kompetens förväntas man som anställd kunna installera och hantera sin egna arbetsstation.

FJÄRRÅTKOMST

Rackfish anställda kan alltid komma åt sin mejl via outlook.rackfish.net eller via sin dator & telefon oavsett var man är så länge man har tillgång till Internet.

All inloggning till våra och våra kunders servrar/tjänster ska ske via VPN när vi inte sitter på det interna nätet.

Utanför EU/EES skall VPN med default route via Rackfish användas.

Access till VPN fås av Rackfish IT.

ANVÄNDARIDENTITER

Det är inte tillåtet att använda resurskonton eller andra gemensamma användaridentiter på grund spårbarhet och den säkerhetsrisk detta innebär. Undantag för denna regel skall beslutas av CTO och endast användas restriktivt där det är motiverat.

HANTERING AV ARBETSSTATION

En bärbar dator kan innehålla mycket känslig information och är stöldbegärlig. Din bärbara dator får inte lämnas synlig i bilen eller obevakad på andra platser där den lätt kan bli stulen.

Det är inte tillåtet att arbeta med känslig information i miljöer där det är möjligt för utomstående att läsa bildskärmen.

Hårddisk på dator skall vara krypterad.

Dator får inte lämnas olåst utan skall vara utloggad eller låst även när den lämnas kortare tid.

UTSKRIFTER

Utskrifter skall användas restriktivt. I det fall utskrifter innehåller känslig information eller personuppgifter skall dessa förvaras säkert och förstöras så fort arbetet tillåter detta.

Vid utskrift av känsligt information är det inte tillåtet att göra det på en skrivare där man inte kan kontrollera att obehörig ej får tillgång till utskriften.

SEKRETESS

All personal är bunden av sekretessavtal som en del av anställningen.

Eventuella frågor på denna policy kan besvaras av CTO.