ANVÄNDAR-HANDLEDNING FÖR VINCI-KONCERNENS INFORMATIONS-SYSTEM

JUNI 2018

INNEHÅLL

Endast den franska versionen av detta dokument är bindande till VINCI Group.

INLEDNING

Informationssystemen är avgörande för att säkerställa att företaget fungerar korrekt och effektivt. På grund av stora risker kopplade till konkurrens, ekonomi, juridik och publicitet, som kan bero på sabotage, bristande vaksamhet eller otillbörlig användning, måste användarnas medvetenhet och ansvarstagande öka, och skydds- och kontrollmekanismerna måste stärkas.

Inom dessa ramar definieras följande i användarhandledningen:

- allmänna regler för användning av resurserna i informationssystemet,
- förbud och punkter att vara uppmärksam på gällande all sorts information, alla typer av uppgiftshantering, alla delar i informationssystemen, alla kommunikationsverktyg och all utrustning som tillhandahålls av företaget,
- skydds- och kontrollprinciper som kan införas.

Användarhandledningen preciserar alltså användarens rättigheter och skyldigheter i samband med användning av informationssystemets resurser.

Handledningens tillämpningsområde

Handledningen gäller alla användare av resurserna i företagets informationssystem.

Med ”användare” avses var och en som, oavsett position (exempelvis anställda, vikarier, praktikanter, konsulter, leverantörer) som använder dessa resurser.

Med ”resurser” avses:

- alla typer av utrustning i informationssystemet (exempelvis datorer, programvara, utskriftsenheter, interna nätverk, delade servrar, flyttbara lagringsmedia),
- alla typer av kommunikationsmedel,
- information och uppgifter (exempelvis filer och databaser).

Alla dessa resurser som står till förfogande för de anställda samt deras innehåll är företagets egendom.

Användarhandledningen tillämpas i alla de länder där koncernen har verksamhet. Den kan kompletteras vid behov, med tillägg som anpassas till de speciella förutsättningarna i varje land och vid varje enhet.

Allmänna regler för användning av resurserna

Tillgång till resurserna

Tillstånd för tillgång till resurserna utfärdas av företaget till varje användare utifrån dennes roll och uppdrag.

Dessa tillstånd är strikt personliga och kan av princip aldrig på något sätt och inte ens tillfälligt överlåtas, lånas ut eller överföras till en tredje person, inom eller utanför företaget.

Förändring av användarens anställningsstatus kan medföra förändring av tillstånden.

Alla nya tillstånd måste föregås av en speciell ansökan i enlighet med gällande förfaranden.

Tillstånden kan avbrytas, förändras eller dras in i enlighet med säkerhetsförfaranden och förfaranden för tillträdeshantering, bland annat om risk för störningar i informationssystemen upptäcks.

Alla tillstånd upphör då yrkesverksamheten avbryts eller upphör, och senast då anställningskontraktet bryts.

Princip för resursanvändning

Resurserna ställs till användarnas förfogande för yrkesmässig användning inom ramen för deras befogenheter enligt det uppdrag som har lämnats dem inom ramen för deras anställning.

Alla dessa resurser samt deras innehåll är företagets egendom. Användaren är ändå ansvarig och bidrar inom sitt område till deras säkerhet.

Användningen av dessa resurser får inte leda till ifrågasättande av företagets ansvarstagande eller skada dess anseende.

Vidare får dessa resurser aldrig:

- användas för att driva personlig affärsverksamhet,
- hindra eller begränsa yrkesmässig användning av företagets resurser, dess underhåll eller säkerhet (inklusive sekretess, tillgänglighet eller integritet).

Användaren får under inga omständigheter ägna sig åt någon lagstridig verksamhet eller verksamhet som skadar företagets anseende eller säkerheten, integriteten eller prestandan i företagets informationssystem.

Rätt till utloggning

Bestämmelserna för rätt till utloggning nedan avser att öka medvetenheten och ansvarstagande hos användarna.

Användarna uppmanas* även att:

- undvika att skicka e-post och SMS samt ringa telefonsamtal utanför ordinarie arbetstid,
- använda sig av funktionen fördröjd leverans av e-postmeddelanden, i förekommande fall samt om e-postklienten tillåter det,
- ange sista svarsdag i sitt meddelande,
- upplysa om att de inte är tillgängliga via ett frånvaromeddelande, och om möjligt skicka vidare ärendet till en tillgänglig medarbetare,
- avaktivera e-postaviseringar utanför ordinarie arbetstid.

Användarna påminns också om att det inte är obligatoriskt att besvara e-postmeddelanden, SMS eller telefonsamtal utanför ordinarie arbetstid*.

Slutligen vill vi understryka vikten av att ledningen är förebilder när det gäller rimlig och genomtänkt användning av de digitala verktygen.

Användning av internettjänster

Tillgång till internet tilldelas användarna individuellt och ställs till förfogande för yrkesmässig användning. Den är inställd och administreras i detta syfte.

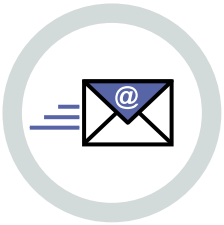
För att inte sänka den allmänna säkerhetsnivån ska användaren vid användande av internettjänster visa respekt för lagar och de regler som gäller på besökta hemsidor.

Han/hon får inte:

- koppla upp sig eller försöka koppla upp sig på något annat sätt än via den officiella internettillgången som tillhandahålls genom företagets nätverk,
- besöka sidor som kan utgöra en säkerhetsrisk för resurserna eller skada informationssekretessen,
- allmänt använda internettjänster i affärsdrivande syfte, för spel eller i olagligt syfte.

* Utom i särskilda fall, exempelvis vite.

Vi påminner vidare om att varje anställd under arbetet i enlighet med sitt anställningskontrakt har lojalitetsplikt. Denna skyldighet tillämpas också på offentliga internetplatser och särskilt på bloggar, forum och sociala medier. Det är strängt förbjudet att på denna typ av sida, på sociala medier eller på internet överhuvudtaget röja information som tillhör företaget eller som skadar dess renommé.



Användning av e-postsystemen

Tillgång till företagets e-postsystem tillhandahålls användarna för yrkesmässig användning. Den är inställd och administreras i detta syfte.

Av tillgänglighetsskäl och av resursprestandaskäl måste meddelandena vara begränsade i volym och antal. Ledningen för informationssystem förbehåller sig rätten att begränsa den maximala storleken på meddelanden, inkorgar och vissa typer av bifogade filer.

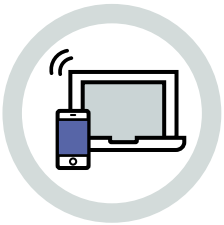
Vid utskick av ett meddelande måste särskild hänsyn tas till mottagarlistans relevans samt till meddelandets utseende, innehåll och storlek.

Användaren ska vinnlägga sig om att tillämpa följande regler:

- tydligt skriva meddelandets ämne,
- använda interna och externa sändlistor med försiktighet,
- vara särskilt noga med all kommunikation av personuppgifter (se paragrafen Om personuppgiftsskydd, s. 10),
- att inte skicka vidare internt meddelanden som kan innehålla virus (vid tveksamhet, kontakta ledningen för informationssystemen),
- att inte skicka ut ur nätverket meddelanden eller bifogade filer med sekretessbelagt innehåll (vid behov, kontakta ledningen för informationssystemen) eller som kan skada företagets rykte,
- att inte sprida adresslistor eller organisationsscheman utanför koncernen.

Om mottagande av meddelanden:

- alla tveksamma, icke legitima och icke önskade meddelanden (avsändare och domänadress okända, meddelanden utan ämne, värvningsförsök eller sedlighetssårande innehåll osv.) ska raderas utan att öppnas, och utan att klicka på länkar eller bifogade filer,
- användaren ska vara särskilt försiktig vad gäller prenumerationer på offentliga sändlistor, som ofta utgör källor till oönskade reklammeddelanden (spam) och spridning av virus genom identitetsstöld.



Rörlighet

Användare av bärbara datorer och alla typer av mobila enheter ska noggrant säkra och skydda sitt material och tillgången till de uppgifter de innehåller, oavsett var de befinner sig, inom eller utom landet, och specifikt vid individuell eller kollektiv transport.

Om utrustning från informationssystem försvinner efter förlust eller förmodad eller påvisad stöld, måste användaren meddela ledningen för informationssystem med alla till buds stående medel och så fort som möjligt, så att nödvändiga åtgärder kan vidtas för att skydda företagets informationssystem.

Samtidigt ska han också rapportera händelsen till sina överordnade så att en bedömning av den potentiella skadan för företaget kan göras.

Vid uppkoppling till företagets nätverk från en allmän plats eller en arbetsplats som inte tillhör företaget ska användaren se till att inte registrera sitt lösenord för uppkoppling från webbläsaren, att logga ur från alla öppna sessioner, att radera surfhistoriken samt att stänga de program som har hjälpt honom att koppla upp sig.

Användaren ska också se till att inte lagra yrkesrelaterad information på någon annan utrustning än den som har tillhandahållits honom av företaget.

Alla användare ska slutligen koppla upp sin bärbara dator mot företagets nätverk så regelbundet som möjligt så att underhållsoperationer samt uppdatering av skyddsprogram görs i enlighet med företagets säkerhetspolicy eller den goda praxis som finns på området.

Materialens, programmens och applikationernas överensstämmelse

Material

För att säkerställa optimal överensstämmelse mellan individuella enheter (datorer, arbetsstationer osv.), informationssystemets applikationer och nätverket tillhandahåller företaget standardkonfigurationer. Föregående validering från ledningen för informationssystemen är även obligatorisk vid installation av utrustning som inte har tillhandahållits, även om det är material som är helt identiskt med det som redan har använts.

Flyttbara lagringsmedia (såsom USB-minnen eller externa hårddiskar) kan vara inkörsportar för virus på arbetsposter och nätverket. Det är obligatoriskt att använda sådana med försiktighet, särskilt när de kommer från utanför företaget. Vid tveksamhet ska användaren kontakta ledningen för informationssystemen som utför adekvata säkerhetskontroller.

Med tanke på att de är små, vilket gör att de lätt kan tappas bort eller stjälas, är det också viktigt att ta bort filerna från dem när överföringen av data är klar.

Slutligen ska användaren om det inte finns någon tidigare definierad konfiguration för ett specifikt behov vända sig till ledningen för informationssystemen för att undersöka vilken lösning som skulle vara bäst för att lösa det behov som har kommit till uttryck.

Utlåning och återförsäljning av material

Det är förbjudet att låna ut, sälja eller överlåta utrustning som har tillhandahållits av företaget till tredje person.

Program och applikationer

Programvarukonfigurationer definieras av företaget för att uppfylla användarnas behov. Alla försök till förändring av ursprunglig konfiguration är förbjudna, eftersom detta kan framkalla allvarliga funktionsstörningar i resurserna (påverkan på prestanda, säkerhet osv.).

Om det inte finns någon förutbestämd konfiguration för ett specifikt behov måste användaren vända sig till ledningen för informationssystem för att undersöka vilken lösning som skulle vara bäst för att lösa det behov som har kommit till uttryck.

För att garantera hög säkerhet och prestanda är det förbjudet att blockera de automatiska processerna för uppdatering av programvaran.

Individuell IT-utveckling

Ansvaret för IT-utveckling utifrån kontorsautomation (makron, databaser osv.) och ansvaret för dess underhåll ligger helt och hållet på användarna som har initierat dem.

Utlåning och återförsäljning av programvara eller licens

Enligt lagstiftningen om immateriella rättigheter åtjnuter företaget användar- och licensrätt till programvaran.

Det är alltså förbjudet att till tredje person låna ut, sälja eller överlåta programvara, licenser, installationsprogram och verktyg som har tillhandahållits av företaget. Detta förbud gäller också programvara som har utvecklats av IT-team inom företaget.

Säkerhet och uppgiftsskydd

Alla användare deltar i säkerhet och skydd av resurser, särskilt uppgifter som hanteras, och åtar sig att inte avsiktligen kringgå, störa, hindra, avbryta eller radera säkerhetsanordningar (antivirusprogram osv.), samt anordningar för filtrering eller kontroll som företaget har infört.

Användaren måste meddela ledningen för informationssystem så fort som möjligt vid konstaterad funktionsrubbning eller upptäckt avvikelse, såsom intrång i informationssystemet osv. Han måste också meddela sina överordnade vid möjlig tillgång till en resurs som inte motsvarar hans behörighet.

Om e-post och internet

E-postsystemet är inte en säker kommunikationskanal om ett meddelande skickas till någon utanför företaget.

Företaget kan kontrollera sitt interna nätverk, men har ingen insyn eller handlingsmöjlighet när uppgifter överförs på det allmänna internetnätverket. Därför bör känsligheten i uppgifterna bedömas innan de överförs till tredje person utanför företaget med detta kommunikationsmedel.

Skyddsmekanismer för kontorsfiler som omfattar lösenord som har föreslagits i redigeringsapplikationer (Word, Excel, Powerpoint, PDF osv.) ger inte något effektivt skydd, med tanke på att det finns många program fritt tillgängliga på internet som gör att de lätt kan kringgås.

Om användaren av yrkesmässiga skäl måste utbyta särskilt känslig information med en tredje person utanför företaget, så ska han/hon vända sig till ledningen för informationssystem på sin avdelning för att få en lösning som är anpassad till de förväntade sekretesskraven och kompatibel med företagets resurser.

När företaget enligt lagen måste införa ett system för loggning* och filtrering** av internettillgången, e-postsystemet och de uppgifter som skickas kommer företaget att lämna begärda uppgifter till behöriga kontrollmyndigheter.

Om användning av krypterade lösningar

Användaren ska endast använda av företaget godkända lösningar för att skydda sina uppgifter.

Om skydd av arbetsplatsen

Tillstånd för tillgång till resurserna, däribland arbetsplatsen, utfärdas personligen till namngiven användare. Alla användare ska i detta sammanhang, för att skydda tillgången gentemot tredje person, vem det än må vara, inklusive i enskilda fall:

- tillämpa företagets policy gällande lösenord (förnyelse, tillräcklig längd, komplexitet osv.) för tillgång till resurserna,
- hålla de lösenord hemliga som absolut inte får överlåtas, lånas ut eller överföras på något sätt till tredje person vare sig inom eller utanför företaget, inte ens tillfälligt (om det inte är absolut nödvändigt av tjänsteskäl, och i så fall ska lösenordet ändras),
- låsa sin arbetsplats när han/hon inte är där och stänga av den i slutet av dagen och över helgen, förutom vid tekniskt underhåll av resurserna eller av driftsskäl,
- inte utnyttja och/eller offentliggöra eventuella säkerhetsluckor som rör de resurser som står till förfogande för honom/henne som han/hon känner till. Ledningen för informationssystemen ska informeras om detta snarast möjligt,
- inte försöka kringgå eller blockera de skyddssystem som är installerade på arbetsposterna (antivirusprogram, brandväggar osv.),
- använda de medel som har ställts till hans/hennes förfogande av företaget för att säkra arbetsposterna,
- utföra skyddsåtgärder på sin arbetsplats. Informera ledningen för informationssystemen vid funktionsstörningar.

Fjärrstyrning av en användares session kan bara utföras då användaren dessförinnan har bett om assistans, eller efter begäran från ledningen för informationssystem och med tillstånd från berörda överordnade. Endast personal som av företaget har getts behörighet har tillstånd att göra ingrepp i de resurser som står till användarnas förfogande.

* Teknisk inloggningsinformation såsom tidpunkt för tillgång och användarens IP-adress sparas.

** Införandet av filtrering för tillgång till webbplatser kräver vid behov avkodning av de uppgifter som har utbytts mellan användarposten och webbplatsen. Detta är en helhetsanalys. De avkodade uppgifterna registreras inte (ej tillgänglig information). Loggning av avkodade flöden motsvarar den som har konfigurerats för standardiserade HTTP-flöden (tidpunkt, användarkonto, internetsidans URL, tillträdestillstånd, identifierat virus). Ingen annan information registreras.

Om kontinuitet i verksamheten

Användare som är frånvarande måste av kontinuitetsskäl använda nödvändiga delegationer som ger tillgång till hans arbetsrelaterade information och får inte lämna sina egna tillträdeskoder till tredje person.

Användaren ska därutöver regelbundet spara och arkivera de uppgifter som han/hon hanterar, skapar eller förändrar för tjänstens kontinuitet genom att använda programvara, material och/eller processer som har ställts till förfogande av företaget, bland annat nätverksplatser.

När användarens verksamhet upphör ska han/hon återlämna till företaget det material som har lämnats honom/henne samt akter, register, filer, e-postbrev och alla arbetsrelaterade elektroniska dokument, för att säkerställa kontinuitet i verksamheten.

Om personuppgiftsskydd

Användarna kan under yrkesutövningen få tillgång till personuppgifter (om anställda, potentiella kunder, kunder, samarbetspartners...) och är medvetna om att dessa uppgifter är sekretessbelagda.

Med ”personuppgifter” avses varje upplysning som avser en identifierad eller identifierbar fysisk person. En ”identifierbar fysisk person” är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en indentifierare såsom ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Användarna ska följaktligen vidta alla nödvändiga åtgärder inom ramen för deras befogenheter för att skydda sekretessen för den information som de har tillgång till, framför allt genom att förhindra att den sprids till personer som inte har uttryckligt tillstånd att ta del av den informationen.

Användarna uppmanas även att:

- inte använda, återge eller utnyttja personuppgifter som de har tillgång till i andra syften än det som avses i deras befogenheter,
- inte röja dessa uppgifter för annan än personer som på ämbetets vägnar är bemyndigade att få dem kommunicerade, vare sig det är privatpersoner, offentliga personer, fysiska eller juridiska personer, och i de fall som uttryckligen anges i företagets förfaranden,
- inte göra någon kopia av dessa uppgifter, såvida det inte är absolut nödvändigt för utförande av deras arbete,
- vidta alla lämpliga åtgärder inom ramen för deras befogenheter för att undvika felaktig eller bedräglig användning av dessa uppgifter,
- så snart som möjligt informera sina överordnade om all kommunikation till icke bemyndigad tredje person, förlust, förstörelse och oavsiktlig ändring av personuppgifter,
- vidta alla åtgärder, däribland säkerhetsåtgärder, för att bevara dessa uppgifters fysiska och logiska säkerhet (exempelvis krav på att skriva in användarnamn/lösenord och att hålla lösenordet för tillgång till resurserna hemligt).

Kontroll av användning av resurserna

Företaget förbehåller sig möjligheten att genomföra regelbundna kontroller i enlighet med principerna för transparens och proportionalitet, i säkerhetssyfte för kontroll av god tillgång till företagets resurser, för att informationssystemet ska fungera bra och för att undvika straffrättsligt eller civilrättsligt ansvar då användarna använder dess resurser.

Av dessa skäl inför företaget filter- och kontrollanordningar (bland annat brandvägg, system för kontroll av tillgång och system för spårbarhet) och säkerställer att dessa fungerar bra, vad gäller användning av företagets resurser (bland annat Internet, e-postsystemet, gemensamma nätverksservrar samt fast eller mobil telefoni).

Dessa system kan införas, bland annat e-post, för att kontrollera alla inkommande eller utgående meddelanden (antivirus-kontroll, antispam-kontroll, integritetskontroll, storlekskontroll, lista över mottagare osv.) och även för att framför allt utifrån en lista över nyckelord blockera meddelanden, elektroniskt utbyte eller tillgång till icke tillåtna webbplatser.

Införande

Spridning

Varje enhet inom Koncernen kan ta initiativ till att sprida föreliggande dokument.

Respekt för gällande lagar

Inom ramen för användningen av de resurser som har ställts till användarens förfogande åtar sig användaren att följa denna handledning, samt att respektera de lagar och regler som gäller i hans/hennes land.

Påföljder

Om de regler och åtgärder som förekommer i denna handledning inte följs kan användaren hållas personligen ansvarig, eller om det rör sig om en konsult, kan företaget som har anlitat denne hållas ansvarigt. Så snart det är bevisat att förseelserna kan tillskrivas honom/henne personligen kan användaren utsättas för eventuella disciplinära påföljder enligt interna regler, eller bli föremål för rättsliga åtgärder i enlighet med tillämplig rätt.

VERKLIGA
FRAMGÅNGAR
ÄR DE MAN
DELAR
MED ANDRA

Upplaga juni 2018 - GSI-2018-06-SV - foto: rawpixel.com från Pexels - Design: www.gcommeuneidee.com

VINCI
1, cours Ferdinand-de-Lesseps
92851 Rueil-Malmaison Cedex
Tel. + 33 1 47 16 35 00
www.vinci.com