

Retningslinjer for oppførsel og akseptabel bruk

Banijay skal beskytte Banijay, sine ansatte og sine kunder mot tap, tyveri, misbruk og uautoriserte handlinger.

Denne policyen fastsetter reglene for ansattes oppførsel med tanke på bruk og beskyttelse av informasjon, våre eiendeler og ressurser i sammenheng med Banijays verdier, som er beskrevet i vår Code of Conduct.

Vi

Skal ikke bruke informasjon og ressurser på en måte som slår negativt ut på andre mennesker eller selskapet vårt.

Du

Er ansvarlig for å beskytte og bruke all informasjon og alle ressurser du trenger i jobben din på en passende måte.

Sammenheng

Denne policyen bør leses i sammenheng med de andre delene av vårt Information Security Policy Framework, som gir mer spesifikke regler for å sikre informasjonssikkerhet i Banijay.

Vi setter pris på tilbakemelding på dette dokumentet. Send den til [**CRT@Banijay.com**](mailto:CRT@Banijay.com).

Etterlevelse

Brudd på denne policyen, med eller uten overlegg, vil bli behandlet i henhold til våre disiplinære prosedyrer. I alvorlige tilfeller vil policybrudd bli ansett som tjenesteforsømmelse og vil kunne føre til oppsigelse og muligens rettslige skritt.

Ikke slutført

I denne policyen kan det hentydes til policyer, standarder og prosedyrer som fortsatt ikke er slutført, disse er markert med **grå tekst**.

Hvem er ansvarlig for hva?

Alle som jobber for Banijay, skal følge vår Code of Conduct og gjøre sitt ytterste for å beskytte vår informasjon, våre eiendeler og våre ressurser.

- Du må kjenne alle deler av denne policyen og oppføre deg deretter.
- Et obligatorisk Banijay-treningskurs om denne policyen er / vil være tilgjengelig.
- Du skal rapportere enhver mistenkelig aktivitet, i henhold til seksjonen "Reporting of Incidents".
- På din siste arbeidsdag før du slutter i selskapet plikter du å levere tilbake all informasjon, eiendeler eller ressurser som selskapet har stilt til rådighet men du har jobbet for oss.

MediArena 1, 1114 BC
Amsterdam, The Netherlands

Shepherds Building Central
Charecroft Way, London, W14 0EE

5 rue François 1er
75008 Paris, France

Banijay

Policyinnhold

Policy

Bruk av selskapets ressurser

Akseptabel bruk

Når du bruker enheten din, kan du:

- Bruke enheten innenfor grensene av etisk og profesjonell oppførsel. Samarbeide med jobbrelaterte kontakter og delta i diskusjonsgrupper som omhandler jobbrelaterte temaer.
- Bruke selskapets maskinvare og nettverk bare til jobb. Men du kan bruke e-post og internettsurfing hvis det ikke bryter med selskapets aktiviteter, forstyrrer driften eller påfører oss ytterligere kostander, og det ikke går utover din egen jobbinnsats eller forstyrrer andre.

Uakseptabel bruk

Når du bruker selskapets utstyr eller personlig utstyr i jobbsammenheng, kan du ikke:

Bruke våre informasjonsverdier til egen vinning på en måte som skader Banijay.

Opptre feilaktig på våre vegne eller gi feilaktige utsagn som vil skade vårt renommé.

Gå inn på, se på, laste ned, laste opp, skape, promotere eller distribuere materiale som kan skade selskapet, som:

- Ulovlig materiale.
- Materiale som oppfordrer til hat eller diskriminering.
- Injurier, misbruker eller trakasserer kolleger, ledelse eller partnere.
- Materiale som inneholder noe av det følgende: pornografi, kjedebrev, nettsider med rase- og hatpropaganda, uautoriserte fellesmailer, spam, ondsinnet programvare, malware eller hacker/cracker-verktøy. – Såfremt det ikke er direkte relatert til og nødvendig for en spesiell produksjon (I disse tilfellene må den lokale IT-avdelingen få beskjed i forkant).

Fører til sikkerhetsbrudd, treghet eller avbrudd i våre IT-systemer og/eller nettverkssystemer eller nettsteder. For å holde denne risikoen på et minimum, kan du ikke:

- Endre på IT-enheter eller hardware, eller endre standardkonfigurasjonen på våre systemer eller informasjonseideler.
- Hacke eller låse opp (jail break) enheter. Bruk av uoffisiell programvare på våre enheter er strengt forbudt.
- Laste ned eller installere tredjepartsprogramvare uten godkjenning av din lokale IT-avdeling.
- Omgå eller redusere noen av våre eller våre partners sikkerhetsmekanismer.
- Bruke noen form for inntrenging, unnvikelsesteknikker, nettverksovervåking eller skanning utover våre normale oppgaver.

Policy

Personvern	Personlig informasjon	Som selskap ønsker vi å sikre all personlig informasjon. Det betyr at personlig informasjon må anses som konfidensielt. Kopiering, deling eller bruk av personlig informasjon må godkjennes av den det omfatter. Hvis du er i besittelse av noen andres personlige informasjon som du ikke trenger i jobben din, må du rapportere det som en sikkerhetsbrist. See Banijay European Data Protection Policy for mer veiledning om å sikre personlig informasjon.
	Brukerpersonvern	For å sikre at vi opptre ansvarlig som selskap, lagrer vi all elektronisk kommunikasjon sentralt og kan overvåke enhver bruk av våre systemer og elektronisk kommunikasjon. Der vi oppfordrer til privat bruk av selskapets enheter, skal lokale regler innføres for å etterleve personvernet..
Sensitiv informasjon (vår ikke-offentlige informasjon)	Hvem kan vi dele med	Vi må holde sensitiv informasjon innad i selskapet vårt. Derfor får du ikke dele sensitiv informasjon med uautoriserte individer. Tilgang til sensitiv informasjon må bli gitt deg ved behov. Du får ikke publisere sensitiv informasjon på offentlige nettsteder eller interne nettsteder som er tilgjengelige for brukere som ikke har et legitimt behov for å ha tilgang til denne informasjonen.
	Sosiale medier	Sosiale medier representerer oss som selskap, vennligst framstill oss på en positiv og akseptabelt måte. Du skal ikke: • Diskutere ikke-offentlig selskapsinformasjon eller annet konfidensielt materiale du jobber med eller har jobbet med for oss; • Lage selskapsspesifikke profiler på sosiale medier uten godkjenning fra kommunikasjonsavdelingen din; • Legge ut, poste eller publisere diskriminerende utsagn, legge ut informasjon eller delta i aktiviteter som kan ærekrenke, skade eller påvirke ryktet vårt eller ryktet til tredjeparter som samarbeider med oss. Dette inkluderer nettoppførsel både i og utenfor arbeidstid; • Bruke interne og eksterne sosial nettverk og fora på en uansvarlig måte; • Bruke selskapskontoen vår til å registrere deg på sosiale nettverk og/eller eksterne fora, med unntak av visse profesjonelle fora.
	Utskrifter	Ikke all selskapsinformasjon er relevant for alle som jobber for selskapet vårt. For å holde informasjonen hos de som har behov for den, må du straks fjerne utskrifter med sensitiv informasjon eller personlig informasjon. Vennligst kvitt deg med disse dokumentene ved hjelp av de rette søppelbøttene eller makulatorene.
Copyright og beskyttet materiale		Som selskap ønsker vi å ivareta eiendomsrettighetene til åndsverk. Dette betyr at uautorisert bruk/lagring av kopibeskyttet og lisensiert materiale, inkludert musikk, videoer, blader, programvareinstalleringer og bilder, på våre maskiner/enheter/servere er forbudt.

Policy

Elektroniske meldinger

Denne delen omhandler alle e-poster, meldinger, tekstmeldinger og bruk av sosiale nettverk og bør leses i sammenheng med informasjonen i "Sensitive Information"-delen.

Beskytte selskapsinformasjon

Vi må beskytte selskapets informasjon. Derfor må alle e-poster som sendes eksternt (til andre enn Banijay-adresser) som et minimum inneholde følgende melding (eller lignende tekst tilpasset til produksjonsselskapet):

Ansvarsfraskrivelse

Innholdet av denne meldingen er konfidensielt og kan inneholde personlig informasjon. Den er kun ment for den opprinnelige mottakeren. Hvis du har mottatt denne ved en feil, vennligst gi oss beskjed per e-post og slett denne meldingen fra systemene dine. Ikke kopier, videresend, eller legg ved noen del av denne meldingen til noen. Takk.

I tillegg kan innholdet i denne meldingen være juridisk gradert.

Personlige e-poster

Vennligst hold dine personlige e-poster personlige, og sørg for at de ikke inneholder noe selskapsinformasjon – ikke bruk personlige e-postkontoer når du representerer selskapet, f.eks. aldri bruk din personlige e-post til å sende meldinger på vegne av selskapet.

Selskapets e-post

Vi ønsker å holde informasjonen vår innad i selskapet. Så vennligst ikke bruk selskapets e-postkonto til å motta eller sende personlig e-post. Ikke bruk selskapets e-post til å registrere deg på sosiale medier eller onlineplattformer som ikke er jobbrelevante. Vær spesielt forsiktig når du åpner ukjent e-post fra ukjente kilder som virker mistenkelige, siden det kan føre til cyberangrep som phishing og/eller datavirus.

Auto-forwarding

For å holde informasjonen vår intern, er det ikke lov med auto-forwarding fra selskapets e-postkonto til en ekstern e-post. Ved spesielle tilfeller, kontakt IT-avdelingen din.

Bruk av enheter

Tilgang

For å sikre at uautoriserte personer ikke får tilgang til vår informasjon og ressurser, sørg for at påloggingen din er privat. Bare autoriserte brukere skal ha tilgang på vår informasjon og våre ressurser.

Vi ønsker at våre nettverk skal være sikre til enhver tid. Derfor skal du ikke installere uautoriserte trådløse forbindelser på våre nettverk.

Koble til våre nettverk

Når du jobber eksternt (hjemme, på en flyplass, på et hotell o.l.), må du bruke en autorisert tilkobling til våre nettverk. Enheten din kan ikke være koblet til et kablet og et trådløst nettverk samtidig. Du skal alltid ha Wi-Fi avslått når det ikke behøves. Hvis du jobber eksternt og er sjelden innom våre lokaler, må du koble deg til nettverket minst en gang i måneden via en autorisert ekstern oppkobling. Dette vil gjøre at du kan holde enheten din oppdatert og holde oss trygge.

Policy

Installere programvare	Når du installerer oppgraderinger, vennligst følg lokale prosesser. For shareware, freeware eller trial software trenger du godkjenning av din lokale IT-avdeling før du installerer. Det er ulovlig å installere og distribuere piratprogramvare, inkludert å kjøpe en enkeltlisens og installere den på flere av selskapets enheter. Vær forsiktig med hvilken programvare du laster ned på enheten din (f.eks. WhatsApp støttes ikke av selskapet vårt). Når du installerer programvare, ikke gi tilgang til selskapets e-post, kalender eller annen informasjon.
Tredjeparts programvare	Tredjeparts programvare som f.eks. WhatsApp, Snapchat, Slack og WeTransfer er ikke støttet av oss og kan føre til alvorlige rettslige og reglementsproblemer hvis de brukes i jobbsammenheng. Du kan ikke bruke tredjeparts programvare i jobbsammenheng. Hvis du er i tvil, kontakt IT-avdelingen din. Listen over godkjent tredjeparts programvare er tilgjengelig hos IT-avdelingen.
Overfør data eksternt	Vår informasjon er sikrest når den lagres i selskapets miljøer og systemer. Dette betyr at overføring av data utenfor våre systemer må unngås såfremt det ikke er nødvendig for jobben og det ikke fins andre muligheter (som OneDrive/Box). Dette er spesielt viktig når du vurderer å åpne, kopiere eller lagre sensitiv informasjon på en enhet utenfor selskapet (inkludert private enheter, skylagring, bærbare lagringsenheter eller mobile enheter). Disse er mindre sikre enn selskapets enheter. Eksterne enheter, som eksterne harddisker eller minnepinner, som lagrer personlige eller sensitive data, må være kryptert. Ikke send ikke-offentlige meldinger med sensitiv informasjon via eksterne programmer eller verktøy som ikke er autorisert av oss. Ikke bruk dataoverføringsverktøy du ikke har fått av oss. Se punktet <i>'tredjeparts programvare'</i>.
Personlig bruk av enheter	Vi godtar begrenset bruk av enheter til å sende personlige meldinger, samtaler og nettsurfing. Personlig bruk er et privilegium, ikke en rettighet, og må ikke bli misbrukt. Vi forbeholder oss retten til å begrense eller lukke tilgangen til enkelte telefonnumre eller nettsteder hvis vi anser den personlige bruken for overdrevet eller upassende. Personlig bruk, inkludert sosiale medier (f.eks. Facebook, Twitter, YouTube, o.l.), bør være fornuftig, holdt til et minimum, og bør ikke:: • Oppta mer enn en ubetydelig del av arbeidstiden din; • Gå utover eller kolliderer med jobbrelatert ansvar; og • Bryte noen av våre policyer, inkludert Code of Conduct, Respect at Work Policy og denne policyen. I henhold til loven kan du ikke forvente privatliv eller konfidensialitet i elektronisk kommunikasjon som er produsert, lastet ned, vist, lagret, sendt eller mottatt på våre systemer.
Autoriserte enheter	Bare Banijay Certified Mobile Devices som møter Banijay Mobile Device Security Standard (som en del av Banijay Security Policy Framework) er autorisert til å bli koblet opp på vårt e-postsystem. Mobile Device Security Standard gir deg ytterligere informasjon om sikkerhetskontrollen på alle mobile enheter som er tilknyttet systemet.

Policy

Bruk av mobile enheter	Bruk av personlige mobile enheter	Du har lov å bruke personlige mobile enheter, men det er ikke tillatt å lagre selskapets data på din personlige mobile enhet, såfremt du ikke bruker vår Mobile Device Management (MDM)-løsning. Vi gjør dette for å beskytte selskapets data.
	Dataminimalisering	Vi ønsker å redusere risikoen for informasjonslekkasjer. Siden passord alene ikke beskytter informasjon, ber vi deg om å slette all sensitiv informasjon lagret på dine mobile enheter som kan knyttes til selskapets nettverk. Vennligst slett jobbrelaterte e-poster, apper eller informasjon som ikke lenger er i bruk eller nødvendig.
Beskytte informasjon	Systemoppdateringer	Vi oppfordrer deg til å jobbe med sikre enheter. Derfor ber vi deg om å jevnlig oppdatere og «patche» dine enheter der det ikke gjøres automatisk av IT-avdelingen din.
	Tap eller tyveri	Ved tap eller skade må du se seksjonen «Rapportere et databrudd». Du må kontakte tjenesteleverandøren din til du mottar bekreftelse på at enheten er tømt av ditt lokale Banijay IT-team.
	Innkjøpssystem	IT-ressurser inkluderer: Datamaskiner, laptop, nettbrett, IT-infrastruktur, servere, programvare, mobiltelefoner og tilhørende. Når du blir tildelt en IT-ressurs, er du ansvarlig for den. Du får ikke kopiere eller dele IT-ressursen med andre brukere uten tillatelse fra IT-avdelingen din. Ansatte som trenger en ny eller må erstatte en gammel ressurs må sende en henvendelse til Screen Media. Selskapets IT-ressurser må skaffes til veie gjennom innkjøpssystemet vårt via en lokal henvendelsesprosess. Hvis du er usikker på din lokale prosess, kontakt IT-avdelingen din. Banijay må ha kontroll på alle enheter i sitt interne miljø, så erstatninger må behandles av IT.
Fysisk sikkerhet	Besøkende	Vi vil sikre at folk i våre bygninger bare slipper inn på områder de har godkjent tilgang til. Det betyr at besøkende må følges av deg eller en kollega til enhver tid. Sørg for at ingen følger etter deg inn på et område de ikke har tilgang til.
	Clean Desk	For å sikre at selskapets data forblir hos selskapet, vennligst lås enheten din før du forlater plassen. I tillegg, lagre alt materiale og alle dokumenter, inkludert mobiltelefoner, nøkler, minnepinner og andre verdisaker, i låste skrivebord, skap eller skuffer og slett all informasjon på tavlene for å sørge for en "clean desk". Vennligst slå av enheten din ved arbeidshagens slutt.
Sikkerhetsklarering	Bakgrunnssjekk	For å opprettholde selskapets sikkerhet, foretar vi av og til periodiske bakgrunnssjekker.
Rapportere et (mistenkt) databrudd		Et databrudd er ethvert brudd på sikkerhetsrutinene som fører til tilfeldig eller ulovlig ødeleggelse, tap, endring, uautorisert overføring eller tilgang til personlig data som sendes, lagres eller behandles på annet vis. Det kan skje med elektronisk lagret informasjon, men også på papir (f.eks. arkiver). Et databrudd skjer, for eksempel, når enheter blir stjålet eller mistet, et cyber- eller ransomangrep inntreffer når e-poster med personlig informasjon sendes til feil person. Hvis det inntreffer et databrudd, selv om det bare er en mistanke, må du umiddelbart rapportere ditt lokale IR, HR og Group Cyber Response Team (CRT@Banijay.com). Banijay er forpliktet til å rapportere databrudd til myndighetene innen 72 timer, så det er avgjørende at du melder fra om et mistenkt databrudd umiddelbart!