Information Security Policy

Internal use only - Confidential - Banijay Group

Alle i selskapet vårt har ansvar for å iverksette de rette tiltakene for å holde oss sikre.

Dette dokumentet er den overordnete policyen for vårt "Information Security Policy Framework". Det gir deg den nødvendig kunnskapen du trenger for å holde oss sikre.

Internal use only - Confidential - Banijay Group

Sammenheng

Denne policyen må leses i sammenheng med de andre delene av Banijay Information Security Policy Framework, som gir deg de spesifikke reglene for implementeringen av informasjonssikkerhet i Banijay.

Informasjonsbeskyttelse

Vi må til enhver tid beskytte selskapets verdier. Derfor skal du bare bruke dem i jobbsammenheng. Alle informasjonsverdier, uavhengig av form eller format, som er laget eller brukt i sammenheng med vår drift, må beskyttes på en måte som tilsvarer deres respektive verdi, sensitivitet, hvor kritisk den er og risikoen ved tap eller spredning.

Informasjonsverdi-ansvarlig klassifiserer informasjonsverdien i henhold til klassifikasjonsnivået som er definert for konfidensialitet, integritet og tilgjengelighet. Sikkerhetsrisikoer må identifiseres, prioriteres og håndteres etter informasjonsverdiens klassifisering for å fastslå det passende sikkerhetsnivået.

Internal use only - Confidential - Banijay Group

Hvem er ansvarlig for hva?

- **Informasjonsverdi-ansvarlige**: Du er ansvarlig for å fastslå de passende og tilgjengelige sikkerhetstiltakene for verdien du eier, og sørge for at dette videreføres til sikkerhetsfunksjonen til ditt produksjonsselskap (OpCo).

- **Ledere på alle nivåer**: Du må sørge for at alle brukere under ditt oppsyn kjenner til denne policyen, og at de følger den i alle aktiviteter.

- **Alle** i Banijay: Utfør dine aktiviteter på en grundig og trygg måte når du følger denne policyen.

Internal use only - Confidential - Banijay Group

Hvem og hva gjelder denne policyen for?

Banijay Group Information Security Policy gjelder:

- **Informasjonsverdier** i et internt eller delt dokument i Banijay Group- og/eller produksjonsselskap, inkludert sky. Informasjonsverdier som omfattes av denne policyen, består av Banijay-informasjon, -systemer og –infrastruktur som omhandler IT, inkludert maskinvare, programvare, infrastruktur for internettoppkobling, e-post og mobildata, i tillegg til utskrifter og informasjon på andre formater (også verbal informasjon).

- **Du** betyr alle som jobber i ethvert Banijay-selskap som ansatt, frilanser, konsulent, midlertidig eller fast personale eller alle som har tilgang til våre systemer og elektronisk kommunikasjon.

Internal use only - Confidential - Banijay Group

Policyinnhold

Internal use only - Confidential - Banijay Group

Tilgangsstyring

For å sikre at informasjonen vår bare vises til de som trenger den, skal du bare bruke informasjonsverdiene når dette er nødvendig i arbeidet ditt.

Vi gir deg tilgang når det er nødvendig og i henhold til arbeidsbehov. Ingen skal få tilgang til informasjon uten nødvendig autorisasjon. Flere detaljer om kontostyring finnes i Banijay Account Management Standard.

Informasjonsverdier og -nettverk er delt opp etter konfidensialitetsnivå.

Innehavere av informasjonsverdier er ansvarlige for å iverksette sikkerhetssystemer fastsatt av de grunnleggende sikkerhetskravene eller av informasjonsverdi-ansvarlig.

Informasjonsverdier må beskyttes av kryptering i henhold til klassifiseringen. Mer informasjon om å behandle informasjonsverdier finnes i Banijay Information Handling and Labelling Standard. For mer informasjon om kryptering gå til Banijay Cryptographic Controls and Key Standard.

Internal use only - Confidential - Banijay Group

Enhetssikkerhet

For å holde enhetene våre sikre, må passord på alle jobbenheter og personlige enheter med tilgang til selskapets informasjon byttes jevnlig i henhold til Banijay Password Security Rules Standard*. Kompleksitetsregler for passord er også forklart her.

Enhver enhet som er tilknyttet Banijay-systemer må følge en aktiv Mobile Device Managemen-implementering som vist i Banijay Mobile Device Security Standard (MDM; gjelder, mobiltelefoner, nettbrett og laptoper). Alle laptoper må beskyttes med antivirusprogramvare og brannmur som er aktiv og jevnlig oppdatert.

*Unntak er gitt for Screen Media sine brukere

Internal use only - Confidential - Banijay Group

Fysisk- og miljøsikkerhet

Vi må beskytte selskapets fasiliteter, kontorer, enheter og utstyrsrom som inneholder infrastrukturen vår. Derfor må vi beskytte dem med passende kontrollfunksjoner for fysisk tilgang (for eksempel en kortleser, et stengt skap eller et låst rom), i henhold til Banijay Facility Physical Security Policy.

Du er ansvarlig for å fysisk beskytte all informasjon som er tiltrodd deg. Hvis en av Banijays informasjonsverdier eller en ressurs som inneholder Banijay-informasjon blir mistet eller stjålet, må du melde sikkerhetshendelsen til Screen Media i henhold til Banijay Security Incident Management Standard.

Internal use only - Confidential - Banijay Group

Systemutviklingssyklus

Vi integrerer sikkerhet og personvern i prosjektsstyringssyklusen vår for å sørge for at informasjonsverdiene våre er godt beskyttet.

En prosjektsyklus innebærer: applikasjonsutvikling, oppkjøp, integrering, testing, overlevering, garanti og utvidelser. Sikkerhetskrav må defineres i startfasen av et prosjekt og bli implementert og testet gjennom prosjektet for å sikre at sikkerheten er høyt prioritert for alle involverte.

For personvern viser vi til Banijay GDPR for mer informasjon.

Internal use only - Confidential - Banijay Group

Driftssikkerhetsstyring

Sikkerhetskontrollen og ansvaret i forbindelse med driftsstyringen vår må dokumenteres og må inneholde en oppdeling av plikter. Informasjonsverdienes integritet må opprettholdes gjennom en formell endring av styringsprosessene.

- All teknologi- og applikasjonsinfrastruktur må beskyttes i henhold til våre sikkerhetspolicyer og standarder.
- Tredjeparts programvare og hardware må opprettholdes på et nivå støttet av leverandøren, og må byttes ut når det ikke lenger støttes av leverandøren.
- Oppdateringer må installeres når det behøves for å motvirke sikkerhetshull og sårbarheter.
- Sikkerhetskontrollen som implementeres må overvåkes (teknisk kontroll av IT, prosesskontroll av selskapseierne) og lydlogger må iverksettes.

Internal use only - Confidential - Banijay Group

Sikkerhetshendelser

Jo raskere vi får vite om en sikkerhetshendelse, jo bedre kan vi håndtere hendelse og minimalisere påvirkningen på selskapet.

Sikkerhetshendelser skal rapporteres til Cyber Response Team CRT@banijay.com, Screen Media og til din leder, dokumentert og riktig håndtert i henhold til:

- Banijay Conduct and Acceptable Use Policy
- Banijay Security Incident Management Standard

Informasjonsverdier må beskyttes med sikkerhetskopier i henhold til vår Backup and Restore Standard og minimumskravene definert av produksjonsselskapet.

Internal use only - Confidential - Banijay Group

Ansattsikkerhet

Vi verdsetter et trygt arbeidsted og trygge medarbeidere. For å sikre dette, må alle som begynner hos Banijay gjennom en sikkerhets- og pålitelighetssjekk før de blir ansatt eller leid inn.

Ledere: Du er ansvarlig for å sikre at personer under ditt oppsyn er gjort oppmerksomme på og opplært i selskapets sikkerhetspolicyer i henhold til deres posisjon eller stilling. Du er også ansvarlig for at personer under ditt oppsyn, jevnlig gjennomgår obligatoriske sikkerhetskurs.

Alle: Du er ansvarlig for å rapportere enhver situasjon som kan true selskapets sikkerhet. Reglene presentert i Banijay Information Security og i Conduct & Acceptable Use Policy gjelder alle.

Internal use only - Confidential - Banijay Group

Forretningskontinuitet

Produksjonsselskaper må utvikle, utvise og opprettholde forretningskontinuitetsplaner for deres funksjoner for å motarbeide risiko for et avbrudd i tilgjengelighet av informasjon nødvendig for forretningskritisk drift.

Internal use only - Confidential - Banijay Group

Etterlevelse

Som selskap må vi sørge for at vi har og opprettholder et tilfredsstillende sikkerhetsnivå. Etterlevelse av Banijay Information Security Policy Framework må sjekkes jevnlig med årlige (selv-) evalueringer. Disse evalueringene må brukes for å sikre at sikkerhetskontrollen er på plass, og at den er tilfredsstillende for å imøtekomme identifiserte risikoer.

Tredjeparts (leverandører, konsulenter, o.l.) etterlevelse av Banijay Information Security Policy må evalueres av innkjøper og lokal IT-avdeling (for teknisk input) som er ansvarlig for forholdet. Tredjepartsleverandører må kjenne til denne policyen og følge den.

Hvis tredjepartsleverandør ønsker å se bort fra policyen, er det bare mulig hvis:

1. Lovverket krever det, eller;
2. Basert på risikovurdering av Banijay, etter en Banijay Group Security Exception Management-prosess, som er bekreftet i en skriftlig erklæring, eller;
3. Deres implementerte sikkerhetsnivå er tilsvarende eller høyere enn sikkerhetsnivået spesifisert i Banijay Information Security Policy Framework.

Alle unntak fra denne policyen må godkjennes av policyeieren. Vennligst kontakt Cyber Response Team på CRT@Banijay.com hvis et unntak fra policyen er nødvendig.

Internal use only - Confidential - Banijay Group