DATABEHANDLERAVTALE

MELLOM:

Radøy Kommune, med adresse Radøyvegen 1690, 5936 Manger en kommune registrert i Norge og i Brønnøysundregistrene under nummer 954748634 (heretter: "**Behandlingsansvarlig**"),

OG

Lindorff AS, et foretak registrert i Norge, med forretningsadresse i Hoffsveien 70B, 0377 Oslo og postadresse Postboks 7055, 3007 Drammen, registrert i Foretaksregisteret under organisasjonsnummer 835 302 202 (heretter: "**Databehandler**"),

Heretter "**Part**" og "**Partene**".

ER ENIGE OM FØLGENDE:

1. Hensikten med denne databehandleravtalen

1.1. Denne databehandleravtalen gjelder utelukkende for behandling av Personopplysninger som omfattes av avtale av 1. januar 2015 mellom partene for låneadministrasjon (heretter referert til som "**Tjenesteavtalen**").

1.2. Begreper som "behandling", "personopplysninger", "behandlingsansvarlig" og "databehandler" skal ha den betydning som er tildelt dem ved gjeldende nasjonal gjennomføring av databeskyttelsesdirektivet (1995/46 / EF) eller - fra ikrafttredelse i Norge - Personvernforordningen (2016/679 / EU), sammen med nasjonale lover som er vedtatt som følge av dette, i det følgende: "**Personvernregler**").

1.3. Databehandleren vil behandle personopplysninger (heretter "**Personopplysninger**") på vegne av Behandlingsansvarlig ved sin utførelse av Tjenesteavtalen med Behandlingsansvarlig. En oversikt over kategoriene av Personopplysninger, kategorier av registrerte, behandlingens art og formål som Personopplysningene behandles for, er gitt i Vedlegg 1.

2. Behandlingsansvarlig og databehandler

2.1. Behandlingsansvarlig er «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av Personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett», mens

Databehandler er «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler Personopplysninger på vegne av den behandlingsansvarlige».

2.2. Databehandler garanterer at den kun behandler Personopplysningene på en slik måte - og i et slikt omfang - som er nødvendig for å levere tjenestene i henhold til Tjenesteavtalen, med unntak av behandling i henhold til (skriftlige) instruksjoner fra Behandlingsansvarlig, eller for å overholde juridisk forpliktelse som Databehandleren er underlagt. I slike tilfeller skal Databehandler varsle Behandlingsansvarlig om slik rettslig forpliktelse, med mindre varsel er forbudt i henhold til gjeldende lov. Databehandler skal aldri behandle Personopplysningene for sine egne formål. Databehandler skal sørge for at fysiske personer som handler under Databehandlerens myndighet og som har tilgang til Personopplysninger, er bundet av dette punktet av databehandleravtalen.

2.3. Databehandler skal informere Behandlingsansvarlig omgående dersom Databehandleren mener at en (skriftlig) instruksjon fra Behandlingsansvarlig er i strid med eller forårsaker brudd med denne databehandleravtalen eller gjeldende personvernregler.

2.4. Nærmere bestemt kan Behandlingsansvarlig gi instruksjoner med hensyn til oppbevaringsperioden for Personopplysningene som er angitt i Vedlegg 1.

2.5. Databehandleren skal ha adgang til å utøve skjønn ved valg og bruk av midler som anses nødvendig for å overholde Tjenesteavtalen og de (skriftlige) instruksjonene fra Behandlingsansvarlig. Databehandleren garanterer at de tiltakene som er tatt, til enhver tid gir et tilstrekkelig beskyttelsesnivå.

3. Konfidensialitet

3.1. Uten at det berører eksisterende avtaler mellom partene, garanterer Databehandleren at alle Personopplysninger og dokumentasjon skal behandles som strengt konfidensielt, og at alle ansatte, agenter og / eller godkjente andre databehandlere som er involvert i behandlingen av Personopplysningene skal informeres om den konfidensielle karakteren av slik informasjon og Personopplysninger. Databehandleren skal sørge for at alle slike personer eller parter har inngått en tilstrekkelig konfidensialitetsavtale og / eller er under noen annen bindende taushetsplikt, og skal gi Behandlingsansvarlig kopi av slike avtaler ved forespørsel.

3.2. Partene skal behandle all informasjon om denne databehandleravtalen strengt konfidensielt. Denne bestemmelsen gjelder også etter at avtalen er avsluttet.

3.3. Den konfidensielle karakteren av informasjonen som er beskrevet under punkt 3. Konfidensialitet, er ikke til hinder for at en Part i kan dele denne informasjonen med en tredjepart dersom og i den grad det er obligatorisk i henhold til gjeldende regelverk.

4. Sikkerhet

4.1. Uten at det berører andre sikkerhetsstandarder som er avtalt mellom Partene, skal Databehandleren treffe hensiktsmessige tekniske og organisatoriske tiltak for å sørge for sikker behandling av Personopplysninger. Disse tiltakene skal i alle tilfeller omfatte:

(a) tiltak for å sikre at Personopplysningene kun er tilgjengelig for autorisert personell for de formål som er angitt i Vedlegg 1 til denne databehandleravtalen;

(b) tiltak for å beskytte Personopplysningene mot utilsiktet eller ulovlig destruksjon, utilsiktet tap eller endring, uautorisert eller ulovlig lagring, behandling, tilgang eller deling, særlig ved pseudonymisering og kryptering av data;

(c) tiltak for å gjenopprette tilgjengeligheten og tilgang til Personopplysninger innen rimelig tid etter en fysisk eller teknisk hendelse, for eksempel bruk av sikkerhetskopiering;

(d) tiltak for å avdekke brudd på og mulige sårbarheter i sikkerheten til systemene som brukes til å levere tjenester til Behandlingsansvarlig;

(e) tiltakene regulert i «Intrum Group Information Security Requirements for Suppliers" i Vedlegg 2.

4.2. Databehandleren skal til enhver tid ha en egnet, skriftlig sikkerhetspolicy med hensyn til behandling av personopplysninger, som minst regulerer de tiltakene som er fastsatt i punkt 4.1 i denne avtalen. Databehandleren skal på anmodning fra Behandlingsansvarlig gi en kopi av slik sikkerhetspolicy, samt vise tiltakene den har tatt i henhold til denne avtalens punkt 4, gi Behandlingsansvarlig adgang til å revidere og teste slike tiltak, og skal endre sin sikkerhetspolicy ved eventuelle skriftlige instruksjoner fra Behandlingsansvarlig.

5. Forbedring av sikkerheten

5.1. Partene erkjenner at kravene til sikkerhet er i stadig forandring, og at effektiv sikkerhet, som skal sikre kontinuerlig konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester, krever hyppig evaluering og regelmessige forbedringer av utdaterte sikkerhetsforanstaltninger. Databehandleren vil derfor evaluere tiltakene som er implementert i samsvar med punkt 4 på løpende basis, og vil styrke, supplere og forbedre disse tiltakene for å opprettholde kravene i punkt 4.

5.2. Behandlingsansvarlig har rett til å instruere Databehandleren om å treffe ytterligere sikkerhetsforanstaltninger. Når det er nødvendig med en endring av Tjenesteavtalen for å utføre en slik instruks, skal Partene i god tro forhandle om en endring av Tjenesteavtalen.

6. Revisjon

6.1. Behandlingsansvarlig har rett til å utføre en revisjon av Databehandleren for å avgjøre i hvilken grad Databehandleren overholder bestemmelsene i Databehandleravtalen. Slike revisjoner vil bli utført av en uavhengig tredjepart og vil finne sted på et tidspunkt som er Partene blir enige om. Databehandleren skal gi - på revisors anmodning - gi revisoren tilgang til de fasiliteter, personell, retningslinjer og dokumenter som etter rimelighet er nødvendige for revisjonens formål.

6.2. Behandlingsansvarlig vil bære kostnadene for revisjonen, med mindre revisjonen avdekker at Databehandleren ikke overholder databehandleravtalen. I så fall bærer Databehandleren kostnadene ved revisjonen.

7. Internasjonal dataoverføring

7.1 Databehandleren skal umiddelbart informere Behandlingsansvarlig om eventuelle (planlagte) permanente eller midlertidige overføringer av Personopplysninger til et land utenfor EØS-området og skal bare utføre en slik (planlagt) overføring etter å ha fått samtykke fra Behandlingsansvarlig.

7.2 Behandlingsansvarlig kan stille vilkår for samtykket som omhandlet i punk 7.1, for eksempel vilkår om at overføring bare skal finne sted dersom de relevante bestemmelsene i Personvernreglene er oppfylt, for eksempel gjennom standardklausuler.

8. Plikt til å varsle og til å håndtere hendelser

8.1. Databehandleren skal ved forespørsel fra Behandlingsansvarlig umiddelbart fremskaffe all informasjon som anses for å være nødvendig av Behandlingsansvarlig for å overholde eller bevise at den overholder sine juridiske krav, herunder under alle omstendigheter krav fastsatt i Personvernforordningen (EU) 2016/679 "GDPR" (f.eks. Svare på forespørsler om registrerte Personopplysninger, varsel om brudd på Personopplysninger, gjennomføre konsekvensutredning for personvern og forhåndsforhandlinger med tilsynsmyndigheter mv.).

8.2. Databehandleren skal varsle Behandlingsansvarlig om enhver hendelse med relevans for behandlingen av Personopplysninger og skal besvare enhver rimelig forespørsel om informasjon og gi Behandlingsansvarlig adgang til å reagere på og å iverksette nødvendige tiltak i etterkant av hendelsen.

8.3. Begrepet "hendelse" brukt i punkt 8.2 skal i alle tilfeller omfatte:

(a) klage eller en forespørsel (om informasjon) fra en fysisk person som gjelder Databehandlerens behandling av Personopplysninger

(b) undersøkelse eller beslagleggelse av Personopplysningene av offentlige myndigheter, eller en indikasjon på at dette skal finne sted

(c) brudd på sikkerheten og / eller konfidensialitetsplikten som angitt i § 32 i GDPR eller punkt 3 og 4 i denne databehandleravtalen som fører til tap eller enhver form for ulovlig behandling, herunder destruksjon, endring, uautorisert avsløring av eller tilgang til, Personopplysningene, eller noen indikasjon på slik brudd har funnet sted eller er i ferd med å finne sted.

8.4. Ved en hendelse som omhandlet i punkt 8.3 (c), skal Databehandleren informere Behandlingsansvarlig innen 48 timer etter at hendelsen har funnet sted. Slik melding omfatter: (i) arten av hendelsen; (ii) dato og klokkeslett for hvor hendelsen fant sted og ble oppdaget (iii) (antall) registrerte som er berørt av hendelsen (iv) hvilke kategorier av Personopplysninger var involvert i hendelsen (v) om og i så fall hvilke sikkerhetstiltak - for eksempel kryptering - som ble foretatt for å gjøre Personopplysningene uleselige for alle som ikke skal ha tilgang til disse opplysningene vi) ytterligere opplysninger som er nødvendige for at Behandlingsansvarlig skal kunne overholde sine plikter ved hendelser som fastsatt i Personvernreglene.

8.5. Databehandleren skal til enhver tid ha skriftlige prosedyrer som gjør det mulig å gi umiddelbar respons til Behandlingsansvarlig i forbindelse med en hendelse og å samarbeide på en effektiv måte med Behandlingsansvarlig for å løse hendelsen. Databehandleren skal gi Behandlingsansvarlig en kopi av slike prosedyrer etter skriftlig forespørsel.

8.6. Databehandleren har aldri rett til å varsle Datatilsynet om hendelser, som definert i punkt 8.3.

9. Databehandlerens rett til å engasjere andre databehandlere

9.1. De andre databehandlerne som er opplistet i vedlegg 1, er forhåndsgodkjent av Behandlingsansvarlig. Behandlingsansvarlig gir Databehandleren samtykke til å engasjere andre databehandlere. Databehandler skal underrette Behandlingsansvarlig om eventuelle planer om å inngå avtale med andre databehandlere utover de som er forhåndsgodkjent i vedlegg 1. Behandlingsansvarlig vil da ha rett til å motsette seg slike endringer.

9.2. Samtykke fra Behandlingsansvarlig som beskrevet i forrige avsnitt skal være uten betydning for Databehandlerens ansvar overfor Behandlingsansvarlig for at andre databehandlere overholder sine forpliktelser med hensyn til vern av Personopplysninger - inkludert eventuelle potensielle skader - hos en slik tredjepart i samsvar med punkt 11.

9.3. Samtykke fra Behandlingsansvarlig i henhold til avsnitt 9.1 skal ikke endre det faktum at samtykke alltid er påkrevd i henhold til avsnitt 7 før Databehandleren kan engasjere en annen databehandler i et land utenfor EØS.

9.4. Databehandleren skal sørge for at andre databehandlere er bundet av de samme forpliktelsene som Databehandleren i henhold til denne databehandleravtalen og skal føre tilsyn med at dette overholdes. Databehandleren skal, ved første forespørsel fra Behandlingsansvarlig, gi en kopi av (foreløpig) skriftlig avtale med en annen databehandler. Behandlingsansvarlig skal ha rett til å overvåke og inspisere andre databehandlere i samsvar med denne avtalen.

10. Tilbakelevering eller sletting av Personopplysninger

10.1. Ved avslutning av denne databehandleravtalen, eller etter skriftlig forespørsel fra Behandlingsansvarlig, skal Databehandleren slette eller tilbakelevere Personopplysningene til Behandlingsansvarlig. Databehandleren skal samtidig makulere alle eksisterende kopier av Personopplysningene, med mindre lagring av Personopplysningene kreves av gjeldende lov.

10.2. Databehandleren skal underrette alle andre databehandlere som er involvert i behandlingen av Personopplysningene om avslutning av databehandleravtalen, og skal sikre at alle slike databehandlere enten sletter Personopplysningene eller returnerer Personopplysningene til Behandlingsansvarlig, etter Behandlingsansvarlig sitt valg.

11. Ansvar og erstatning

11.1. Lindorff AS er erstatningsansvarlig overfor Behandlingsansvarlig og skal holde Behandlingsansvarlig skadesløs for ethvert krav, handlinger, tredjeparts krav, tap, skader og utgifter pålagt av Behandlingsansvarlig og oppstår direkte i forbindelse med Lindorff AS sitt brudd på denne databehandleravtalen.

12. Varighet og oppsigelse

12.1. Denne databehandleravtalen skal tre i kraft på samme dato som Tjenesteavtalen og skal opphøre automatisk når Tjenesteavtalen avsluttes.

12.2. Det at denne databehandleravtalen sies opp eller utløper, skal ikke frita Databehandleren fra sine forpliktelser med hensyn til Personopplysninger som ikke (ennå) er returnert eller slettet i samsvar med punkt 10.1 eller fra forpliktelser som er ment å gjelde etter oppsigelsen eller utløpet av databehandleravtalen, inkludert blant annet forpliktelsene som følger av punkt 3, 6, 10 og 11 i denne databehandleravtalen.

13. Diverse

13.1. Ved uoverensstemmelse mellom bestemmelsene i denne databehandleravtalen og Tjenesteavtalen skal databehandleravtalen ha forrang.

13.2. Denne databehandleravtalen er underlagt norsk lov. Eventuelle tvister som oppstår som følge av eller i forbindelse med denne databehandleravtalen, skal bringes for Oslo tingrett.

Signatur :	Signatur:
for og på vegne av Behandlingsansvarlig	for og på vegne av Lindorff AS
Navn: Sveinung Kvamme	Navn: Torkel Sør-Reime
Stilling: Økonomisjef	Stilling: Direktør Credit Services
Dato: 19.11.2018	Dato: 27. juni 2018

Vedlegg 1:

Kategorier av Personopplysninger som skal behandles i henhold til Tjenesteavtalen, kategorier av registrerte, behandlingens art og formålet med behandlingen.

Registrerte

- Låntakere og tilskuddsmottagere
- Medlåntakere og kausjonister

Kategorier av personopplysninger

- Kontaktdata (eks. navn, adresse, telefonnr, e-postadresse)
- Personnummer, lån/tilskuddsnummer, pant-/sikkerhetsdata
- Betalingsinformasjon

Spesielle kategorier av personopplysninger

Helseopplysninger og informasjon om andre sosiale forhold i enkelte tilfeller. Dette kan være notater og kommentarer fra kunder med informasjon om enkeltlåntakere samt informasjon som fremkommer i dokumentasjon som oversendes.

Behandlingsaktiviteter

Personopplysningene vil bli underlagt følgende behandlingsaktiviteter (vennligst spesifiser):

- Opprettelse av lånedokumenter og tilskuddsdokumenter
- Etablerings av sikkerhet for lån og tilskudd
- Utbetaling av lån og tilskudd
- Depotfunksjon
- Administrasjon av lån og tilskudd
    - Utsendelse av terminvarsler
    - Misligholdsoppfølging
        - Utsendelse av purringer
        - Oppsigelse av lån med inkassovarsel
        - Inkasso
    - Føring av reskontro
    - Renteregulering
    - Rapportering
    - Avslutning av lån

Tilbakelevering eller sletting av Personopplysninger

- Ved evt. opphør av avtalen så vil persondata kunne oppbevares for å ivareta dokumentasjonskrav ved evt. reklamasjonsbehandling jfr. gjeldende lov.
    - Dokumentasjon til dette formål kan oppbevares i inntil 1 år etter opphør av tjenesteavtalen.
- Persondata som ikke er relevante for saken vil bli tilbakelevert og slettet.

Godkjente databehandlere, jf. pkt 9.1

Underleverandører

- Fujitsu
- PostNord Strålfors
- Nets AS
- Experian
- Accando AS
- Ambita
- Posten Norge
- eBoks
- Signicat
- BankID Norge
- Vipps AS

Vedlegg 2:

intrum

Intrum Group Information Security Requirements for Suppliers ("Intrum ISRS") – Annex 2

1. INTRODUCTION

The Intrum information security requirements for suppliers ("Intrum ISRS") address information security requirements related to data and information, inclusive personal data, being accessed, transferred or in other way leaving Intrum internally controlled environments to suppliers, such as for outsourcing activities and external cloud services based on risk assessments and regulative requirements.
The Intrum ISRS are based on regulatory and contractual requirements, risk assessments and appropriate best practices. The Intrum ISRS also include the technical controls for secure data processing of personal data as regulated in the GDPR.
The Intrum ISRS address processes, procedures and controls that Intrum require the supplier to implement and adhere to as part of the agreement between Intrum and the supplier.
The supplier shall in addition to the Intrum ISRS adhere to any specific security processes or activities specified in the agreement between Intrum and the supplier.
The purpose of the Intrum ISRS is:

- to provide the suppliers of Intrum a baseline and set of mandatory controls for the purpose of securing IT and information assets
- to protect Intrum's information assets from threats to the confidentiality, integrity and accessibility of data, whether internal or external, deliberate or accidental
- to encourage consistent and professional use of information
- to enable secure information sharing

2. SCOPE

The Intrum ISRS apply for all suppliers providing services to Intrum and its subsidiaries (hereinafter called "Intrum") who have full, partial or temporary access to Intrum's information assets, information systems, networks and/or physical environments, included assets that are maintained by a local or Intrum unit as well as assets maintained by third party suppliers. The Intrum ISRS is intended used as an appendix for supplier agreements, data processing agreements, or as part of other services or situation where requirements on security is nesessary. The supplier will annually update the controls to match the risk as identified by the supplier.

3. INFORMATION SECURITY MANAGEMENT (ISMS)

The supplier shall have a documented Information Security Management System (ISMS) aligned with ISO27001, or a set of policies to that effect, and the supplier shall upon request and reasonable advance notice, provide documentation thereof. Such documentation shall comprise clear statements of the policy, objective and scope of its ISMS, and the procedures and controls in support thereof. The supplier shall actively seek to make any renewed versions available upon any significant revision or change of the above mentioned documents.

The supplier shall have a Code of Practice for Information Security Management which is modelled after ISO 27002:2013, 27011:2008 and 27018:2014 (or subsequent version) standard and controls.
The supplier has a duty to:

- Safeguard hardware, software and information in their care
- Report on any suspected or actual breaches in information security
- Follow the mandatory instructions from Intrum ISRS
- Ensure the confidentiality, integrity and availability of information, consistent with legal and management requirements and obligations
- Ensure that their staff is aware of their information security responsibilities
- Ensure that their staff has had suitable information security training
- Regularly review the access of their employees to ensure that they match their role and responsibilities

Any supplier providing services or assistance to Intrum shall comply with the following baseline requirements, and any additional requirements which may be considered to be of best practice to services being provided, if the requirements are applicable to the services or assistance being provided:

4. ORGANISATION OF INFORMATION SECURITY

The supplier shall appoint a named Security Manager for Intrum, for dealing with security issues. The Security Manager shall have sufficient authority to handle any operational and tactical level security issues, to be responsible for security reporting and to make decisions on behalf of the supplier on these matters.

The Security Manager may appoint a Security Contact for the day-to-day handling of operational and tactical level security issues, as well as reporting, towards Intrum, provided that the Security Contact is also given equal authority to handle any foreseeable operational and tactical level security issues and to make decisions on behalf of the supplier on these matters. Upon Intrum's request and reasonable advance notice, the supplier shall partake in a Security meeting.

The supplier shall ensure, by entering into written agreements with any and all subcontractors utilised for the production, transmission or storage of services or deliverables to Intrum, or for the supplier's operations and infrastructure insofar as it is utilised for, or in conjunction with, the production, transmission or storage of services or deliverables to Intrum, or could conceivably affect the security of said services or deliverables, or Intrum’s information or other assets, that all information security requirements and obligations, to the extent relevant for the supplier’s ability to ensure its compliance therewith, equally upheld by the subcontractors.

5. INFORMATION SECURITY RISK MANAGEMENT

The supplier shall follow up and oversee that information security requirements are effective (in place) and efficient (works as intended). This responsibility covers both organizational and technical measures, and therefore also includes the IT security requirements.

Data and information which is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss or corruption. Data and information may be put at risk by poor education and training, misuse, and the breach of security controls.
The supplier must undertake risk assessments to identify, quantify, and prioritise risks. Controls must be selected and implemented to mitigate the risks identified.

6. INFORMATION SECURITY INCIDENT MANAGEMENT

The supplier shall use a formal Incident management system. The purpose of information security Incident management is to identify, respond to Incidents and to restore normal status of information/IT Systems, minimizing the adverse impact and reduce the risk of similar Incidents occurring.
Information security Incident management shall include Incident management and Problem management.
An incident is a disturbance to an IT system or another event leading to the actual outcome(s) of a business process to differ from the expected outcome(s). It also comprises incorrect configurations that have not yet affected a business process.
The supplier shall have policies to manage incidents arising in the services provided.
Incidents shall be recorded in an incident handling system and categorised depending on the impact and urgency also losses that have arisen in conjunction with the incident shall be documented. There shall be procedures in place to ensure that this information is correct. Reported incidents shall be investigated and diagnosed to assess how the

incidents best are resolved. Solution or workarounds and other relevant information about the incident handling shall be documented before the incident record is closed.
The supplier shall have an incident manager for handling of incidents regarding services provided in a timely manner. Incident management routines shall be coordinated with change management to secure that change procedures are not circumvented. Should an incident exceed pre-set thresholds or severity level it shall be escalated according to the supplier's escalation routines. Incidents classified as major and also threaten the availability of critical business systems, shall be reported to as described below.
For technical IT security related incidents, which can compromise the security in infrastructure and production systems, the supplier shall have documented IT security Incident management process. This process shall be connected to procedures for forensic investigations.
The supplier shall report any significant security incidents, which affects the services without undue delay after the incident was first discovered. This also includes security incidents at sub-contractors.
Examples of security incidents that must be reported include:

- intrusion in an IT System
- spreading of adverse program in the supplier/sub-contractor network
- denial of service attacks
- unavailability affecting the services
- other disruptions in data communication affecting the services
- leakage of data

A problem is an undiagnosed root cause of one or more Incidents. Problem management shall be considered for all severe Incidents or Incidents with high resource consumption in order to produce corrective or preferably preventative solutions. The supplier shall have a manager responsible for a problem management process and shall report according to the supplier's procedures the status of open problems on a regular basis.
Problems shall be recorded in a searchable log containing actions taken during the solution. This shall include a description of workarounds until a permanent solution has been implemented. Before closing a problem, the reporter of the Incident shall confirm that it has been solved. The reporter can also be Intrum.

7. DATA OWNERSHIP AND DATA CLASSIFICATION

A data classification scheme applies, based on the criticality and sensitivity of the data. This classification determines how data should be handled, the level of security that applies to the data and applicable security controls:

A. Public Information: Information specifically intended for publication

B. Internal Information: General information only if not containing items from Classification C or Classification D.

C. Confidential Information: Client Data, Customer/Debtor Data

D. Restricted Information: Personnel Files, Share Price Sensitive Information, Security Data. Restricted information should be available only to as few people in the organization as possible.

8. DATA RETENTION

Data retention shall be based on instructions made by Intrum, if not specified in agreement, data processing agreement etc. agreed between Intrum and the supplier.

9. ACCEPTABLE USE, SECURITY EDUCATION AND TRAINING

The supplier is responsible for its personnel and their actions, and shall have a process for ensuring that personnel working with the Intrum's assets are who they claim to be, i.e. conduct an independent verification of identity upon hiring and that the personell are qualified for the job, has good ethics and high personal integrity. The Supplier shall

upon Intrum's request and reasonable advance notice, make available documentation of the supplier's personnel screening process.

The supplier is responsible for imposing obligations and requirements on any and all employees and other persons (together "personnel") performing tasks and activites with regard to Intrum by ensuring that they are known to, understands and comply to the Intrum ISRS.

All employees shall be imposed to exercise good judgment in accordance with policies, standards, and guidelines, and the obligation on the employees shall at minmum cover the following:

1. Control of assets and information: All personnel must always store information on devices and equipment that is within the control of the supplier or as approved by the supplier. Storage of Intrum information on private or non-Intrum controlled or non-supplier controlled environments, including devices and cloud services maintained by a third party with whom Intrum does not have a contractual agreement, is prohibited.
2. Confidentiality, data protection, and protection of third parties: When hired or engaged, the employees shall receive a confidentiality agreement to be signed, as part of the employment contract. Consultants, service personnel, suppliers and other temporarily hired personnel shall sign a "declaration of confidentiality" prior to the engagement.
3. Travel and working from remote locations: When personnel are working remotely or on travel, security precautions shall be taken into consideration.
4. Email – acceptable use: If confidential or sensitive information must be sent by email, encryption or similar technologies must be employed to protect the information. Personal data that are confidential can be communicated by unencrypted email when consent is given by the person the data concerns.
5. Cloud services – acceptable use: The security and compliance of each data center used by each cloud service must be verified.
6. Instant Messaging – acceptable use: Confidential and restricted and/or business-critical information shall not be exchanged via instant messaging. Only approved instant messaging clients should be used. This applies to both internal and external use.
7. Passwords: The IT systems shall automatically request change to passwords on a regular basis. As many systems as possible shall use the central user directory so the number of different passwords personnel need to handle is limited to the extent possible. If some systems do not have this automatic functionality, the personell's shall change their password regularly with an interval not exceeding three months. Upon suspicion that a password is compromised, the uses shall be obligated to change it immediately. It is not permitted to use another person's username and password, neither is the usage of shared user accounts for end users permitted. The personnel shall not be allowed or obligated, to disclose a personal password because of inquiry of any other person. The personnel shall limit the use of the same password for accessing several systems, as disclosure of a password in one system would then lead to a compromise of multiple systems. The same password must not be used for organisational and personal use. See also Section 15 on passoword policy.
8. Virus Protection And Updates: The personnel shall be obligated to ensure that no attempts are made to disable or over-ride any of the installed software, including anti-malware software, firewalls and automatic updating services.
9. Backup: All information shall be protected by backup systems, to ensure recovery from any business disruptions in case of data loss.

10. INFORMATION SECURITY IN PROJECT MANAGEMENT

Identification and incorporoprateion of information security requirements shall be done at the early planning stage of all projects. In doing so, the risk of new security and compliance problems being introduced into the environment is greatly reduced. It also minimises the risk of project schedule delays and cost overruns when security requirements must be retrofitted into systems and/or contractual agreements late in the process.

Baseline Requirements

- Project risk assessment shall be performed, covering at least below subjects, to identified project risks and issues within project:
    - Identify sensitivity of data that the project involves
    - Identify if there is a need for compliance with legal or regulatory requirements, national or international standards or contractual security and privacy obligations
    - Describe planned data input/output processes
    - Describe plans for data storage and destruction
- Project risk analysis shall be repeated at each project phase transition
- Risk owners shall be identified and actions for risk avoidance, acceptance or mitigation (i.e., contingency plan) shall be identified for these risks by considering cost implications.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

Physical exposures could result in financial loss, legal repercussions, loss of credibility or loss of competitive edge. They primarily originate from natural or man-made hazards and can expose the business to unauthorised access and unavailability of business information.

Physical and environmental security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, unauthorised access, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.

Physical access issues are a major concern within information security. Exposures and possible perpetrators are described below:

- Unauthorised entry
- Damage, vandalism or theft to equipment or documents
- Copying or viewing of sensitive or copyrighted information
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing resources

Possible perpetrators are:

- Former employees
- Interested or informed outsiders such as competitors, thieves, organised crime and hackers
- An accidental ignorant

From an information security perspective, facilities to be protected include:

- Computer rooms
- Operator consoles and terminals
- Tape library, tapes, disks and all magnetic media
- Storage rooms and supplies
- Communication closets
- Telecommunications equipment
- Power sources
- Disposal sites
- Dedicated telephones/telephone lines
- Portable equipment
- Onsite and remote printers
- Local Area Networks

Additionally, system, infrastructure or software application documentation should be protected against unauthorised access. For these safeguards to be effective, they must extend beyond the computer facility to include any vulnerable access points and at organisational boundaries/interfaces with external organisations.

Baseline Requirements

- Facilities such as server rooms shall not be visible or identifiable from the outside; there shall be no windows or directional signs.
- Physical accesses to the server room shall be restricted to individuals who require such access to perform their job responsibilities.
- Environmental threat detection and monitoring mechanisms shall be used in the server rooms. Air conditioning systems shall be established to provide required temperature and humid percentage. Smoke detectors shall be used in addition to fire extinguishers to recover devices with least damage in case of a fire disaster rising from excessive heat and electric issues.

12. ASSET MANAGEMENT

IT assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning levels of sensitivity and criticality to each IT asset and establishing specific security rules, it is possible to define the level of access controls that should be applied to each resource.

The first step in IT asset management is the process of identifying and creating an inventory of IT assets. The inventory record of each asset should include:

- Specific identification of the asset
- Relative value to the organisation
- Loss implications and recovery priority
- Physical Location
- Security and risk classification
- Asset group
- Asset owner

IT asset management should be employed for both software and hardware assets. All hardware devices/software used should be managed (inventory, track, and correct) actively, so that only authorised devices/software are enabled.

Baseline Requirements

- All assets shall be recorded in an asset inventory database which shall contain all systems connected to the network and the network devices themselves should be maintained, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks.
- The information required to ensure that the asset inventory is kept up to date (e.g. physical or logical location of the asset, contact details etc.) shall be provided in the asset inventory database.
- The assets shall be correctly classified, that access controls are defined and periodically reviewed and that vulnerabilities are identified and patched.
- The authorised recipients for the information contained in the IT asset shall be identified and compliance with mandatory controls and handling procedures that are effective based on the classification shall be ensured.
- Periodic reconciliation of assets shall be performed at least quarterly to ensure existence and to detect unauthorised devices; the outcome of the reconciliation should be documented in an ITSM system.
- Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data shall be identified, regardless of whether they are attached to the network.
- A list of authorised software and version should be maintained.

- A software inventory tool should be used to keep track of each of the operating system types in use, including servers, workstations, and laptops. The software inventory tool should track the version of the underlying operating system as well as the applications installed on it.

13. USER ACCOUNT MANAGEMENT

User account management procedures address the requesting, establishing, issuing, suspending, modifying and closing of user accounts and the related user privileges. These procedures apply to all users, including administrators (privileged users), internal and external users, for standard and emergency cases. Rights and obligations related to access to systems and information shall be contractually arranged for all types of users. Regular management review of all user accounts and related privileges shall be in place to ensure that there is no Segregation of Duties conflict and terminated and transferred employees do not have inappropriate access rights.

Specific user account control mechanisms shall be applied which:

- Prevent unauthorised access to data
- Limit access to personnel based on the business need to know principle
- Follow the least privilege principle allowing access only to the information and resources which are essential to perform the intended function
- Have the capability of detecting, logging, and reporting access to any systems or network

Baseline Requirements

- Where technically possible, all accounts shall be authenticated by Active Directory. This applies also to Cloud applications / SaaS solutions.
- User accounts are individual and shall not be shared.
- A review of authorisation privileges assigned to each employee shall be coordinated at least on a bi-annual basis to ensure that access is appropriate for the user's functioning role. Technical system owners are responsible to provide information about current accesses that are to be reviewed. Business owners are responsible to conduct the review, and local unit management team is responsible to support and verify the review. A written report of the completion of this review should be recorded in an ITSM system.
- Administrative privileges shall be minimised and administrative accounts shall only be used when they are required.
- Administrative tasks shall be always performed by using the so called "Admin" accounts.
- Users shall not login to their laptop and/or workstation with their "Admin" account. An extra login step is required before the privileged accounts can be used.
- Administrator accounts shall be forced to change their password according to the default domain policy at first logon and every 60 days.
- Administrator accounts shall be disabled and password must be changed immediately. Disabled Administrator accounts should be removed at least on bi-annual basis.
- External accounts shall be forced to change their password according to the default domain policy at first logon and every 60 days.
- Emergency accounts shall be used only in limited situations (e.g. unexpected technical issues which require a fast action/resolution) and shall have mechanisms in place to allow for traceability to an individual. Credentials shall be stored in a secured manner. Management shall approve usage for a specific purpose prior to the credentials being provided.

14. SEGREGATION OF DUTIES AND ACCESS MANAGEMENT

Key duties and functions shall be appropriately segregated, particularly those duties and functions which when performed by the same individual may result in undetected errors or may be susceptible to abuses which may make exposure to inappropriate risks.

Controls for authorising and administering user access should follow the principle of least privilege. This means that user accounts are provisioned such that the lowest level of user access permissions that the user can have and still complete their job duties.

Baseline Requirements

In order to reduce the risk of inappropriate access or unauthorised access to sensitive information the following objectives must be met:

- A formal user registration and de-registration process shall be implemented in an ITSM system to enable appropriate assignment of access rights.
- Role based access shall be employed where possible and shall be based upon the relevant characteristics of job descriptions and/or assigned business process activities.
- Access rights within a defined role shall follow the principle of least privilege, that is to say provisioning of accounts with the minimal amount of access such that the job duties can still be performed.
- Access rights shall be removed or revised when an employee is either terminated or is repositioned.
- Access rights shall be reviewed on a periodical basis or at least annually.
- Where applicable, two 'Approvers' (four eyes principle) shall approve requests to business systems, information and/or processes. This approval can be implicit in that the first approver submits the request on behalf of the user while the second approver approves it.
- Super user or administrative user access rights shall be granted on a need-to-use basis and where possible, separate administrator accounts shall be used for auditing and traceability.
- Unique user id's shall be used to enable users to be linked to and held responsible for their actions when accessing functionality directly in a system.
- With regards to application, software and code development, in general, privileges should be designed and controls should be implemented so that the person who develops the software is not the same person who puts the application or changes to the application into the production environment.

15. PASSWORD POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of resources. All users, including contractors and vendors with access to company systems, are responsible for selecting and securing their passwords.
Some common methods that attackers use for discovering a victim's password include:

- **Guessing:** The attacker attempts to log on using the user's account by repeatedly guessing likely words and phrases such as their children's names, their city of birth, and local sports teams.
- **Online Dictionary Attack**: The attacker uses an automated program that includes a text file of words. The program repeatedly attempts to log on to the target system using a different word from the text file on each try.
- **Offline Dictionary Attack**: Similar to the online dictionary attack, the attacker gets a copy of the file where the hashed or encrypted copy of user accounts and passwords are stored and uses an automated program to determine what the password is for each account. This type of attack can be completed very quickly once the attacker has managed to get a copy of the password file.
- **Offline Brute Force Attack**: This is a variation of the dictionary attacks, but it is designed to determine passwords that may not be included in the text file used in those attacks. Although a brute force attack can be attempted online, due to network bandwidth and latency they are usually undertaken offline using a copy of the target system's password file. In a brute force attack, the attacker uses an automated program that generates hashes or encrypted values for all possible passwords and compares them to the values in the password file.

Each of these attack methods can be slowed down significantly or even defeated through the use of strong passwords. For this reason, a strong password policy shall be enforced for all systems and users.

Baseline Requirements

- Default passwords are prohibited. Password should be changed immediately from default.

- Unnecessary default accounts shall be disabled before installing a system on the network. This applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, Simple Network Management Protocol (SNMP) (community strings, etc.).
- Where possible, the password policies should be enforced by the main authentication provider (Active Directory) or a related user federation service for cloud applications (SaaS). Strong authentication (two-factor-authentication) shall be used to access confidential and restricted data if these are made available through a web interface or API over an open network.
- The "Password never expires" option is not allowed for any account that is used to logon to any information system.
- In the case of service accounts, automatic expiration can be overridden to ensure service continuity. These accounts should be clearly documented and regularly reviewed if they are still being used. It is not allowed to use service accounts for interactive logon.
- All user Active Directory accounts shall be audited for the "Password never expires" option at least on quarterly basis.
- Temporary passwords must be given to users in a secure manner, with expiration on first use.
- Passwords must be encrypted or hashed when transmitting over networks and in storage.
- Passwords should not contain common phrases (such as password, secret etc.), company name (or abbreviation), parts of user's personal information (such as name, surname) or the account name.
- New passwords should be unique and may not be the same as previous used passwords.
- Passwords must meet the following minimum requirements:
    - Minimum Password History: **24** [1]
    - Maximum Password Age: **60**
    - Minimum Password Length: **10**
    - Password Complexity: Passwords must use at least three of the four available character types:

      -**Lowercase letters**: Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)

      -**Uppercase letters**: Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)

      -**Numbers**: Base 10 digits (0 through 9)

      -**Symbols**: ~!@#$%^&*_-+=` |\(){}[]:;"'<>,.?/
    - Minimum Password Age: **1**
    - Store Password Using Reversible Encryption For All Users: Disabled
- For systems that cannot enforce password policies, a regular manual password change must be performed by end-users in accordance to the password requirements.
- Passwords manager software (like Keepass and similar) can be used for securely storing passwords under the below conditions:
    - Passwords must always be stored in an encrypted form by means of strong ciphers (e.g. AES or Twofish).
    - It is not allowed to store passwords in any form on any system that is not fully managed (e.g. cloud solution, privately owned endpoint, etc.)
    - Team managers must ensure that master passwords and/or certificates of shared password databases are changed immediately when a team member leaves the team or company or does not require access to these passwords anymore for any other reason.

[1] For Active Directory the password history requirement is 24.

16. REMOTE ACCESS POLICY

Remote Access connectivity to resources is required for several types of users, such as internal employees, external consultants and vendors or suppliers. In providing this capability, specific policies and controls should be in place to satisfy business needs as well as security requirements.
External access to networks and resources shall only authenticate users via three channels:

- Remote Access (SSL VPN)
- Remote Access (Citrix Access Gateway)
- Site-to-Site VPN

Remote Access and Site-to-Site VPN gateways shall act as entry points for the network and both be located on the edge of the demilitarised zone which is subject to strict security measures.

Baseline Requirements

- Only users with a valid Active Directory account are allowed to use the Remote Access service.
- Remote Access to data or systems must be kept to the minimum by adopting the need to know principle.
- All remote access must authenticate with at least 2 methods (two-factor-authentication). The minimum mandatory level is by means of username/password and user certificate.
- External users shall be allowed to connect to the network only if their connecting device is configured with an updated Antivirus software and with an Operating System which is still under support and being patched;
- Site-to-Site VPN connections are only permitted when they are terminated and managed via the central firewalling infrastructure provided.
- Site-to-Site VPN connections established with external parties shall be centrally authenticated and authorised by an authentication method like a Pre-Shared Key which shall be securely communicated via SMS between the parties.
- All communication via a Site-to-Site VPN connection shall be properly secured implementing strong encryption and hashing industry standards.
- External parties which are connecting via Site-to-Site VPN shall have access only to the resources defined.

17. SENSITIVE MEDIA DISPOSAL AND TRANSPORT

Controls to prevent access to or loss of sensitive information from computers, disks, and other equipment or media when they are stored, disposed or transferred to an external entity shall be implemented.

The below requirements explain the processes that shall be adopted for re-using or destroying all types of media (e.g. paper documents, hard drives, USB sticks, CD/DVD, etc.) to prevent the disclosure of internal, confidential or restricted information.

Baseline Requirements

- All media that contains data shall be physical destroyed or made unreadable before it is disposed of.
- When appliances, printers or telephones are returned under RMA (Return Merchandise Authorisation) they can't be destroyed. Supplier instructions shall be followed to sanitise the hardware before shipping it back to the supplier. When more detailed instructions are not available the configuration must at least be reset to the factory default where possible.
- Paper that contains internal, confidential or restricted information shall be shredded when not needed anymore.
- CD/DVD that contains internal, confidential or restricted information shall be physically destroyed when not needed anymore.
- Faulty flash memory devices such as USB sticks and memory cards shall be physically destroyed.

18. CHANGE MANAGEMENT

Change control procedures are a part of the more encompassing process referred to as change management and are established to control several types of changes such hardware changes, application changes (e.g. programs, jobs, configurations, parameters, etc.), software patch installation, configuration of various network devices etc. The change management procedures implemented are all based on the Information Technology Infrastructure Library (ITIL) which consists of a collection of best practices designed to standardise the selection, planning, delivery and support of IT services.

The main objective of change management is to ensure that changes are recorded and then evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner and to take necessary corrective actions.

Change requests can come from various sources that include (but not limited to):

- Incident management
- Problem management
- Release management
- Continuity management
- New hire
- Employee leaving
- Requests from customers
- Security management

Baseline Requirements

- Change notifications shall be sent to all relevant stakeholders before and after the change implementation.
- Change preparation, scheduling and operating instructions shall be established.
- The change requestor is responsible for testing and making sure that a proper impact analysis is performed, prior to requesting an approval from the business representative. The impact analysis should contain information about the impact on business processes and other linked assets.
- The risk of adversely affecting the business operation shall be reviewed and a rollback plan shall be developed to back out of the changes, depending on the risk level. Predefined risk levels can be applied for different categories of changes.
- A change workflow which includes business representative approval shall be in place.
- Legal and/or compliance aspects shall be considered before implementing a change.
- The change requestor shall verify that the change has been implemented successfully and no other issues were introduced as a result of the change implementation.
- Whenever the change means adding, removing or modifying an information asset, the requestor must verify the asset information in the asset inventory database to make sure the information is still accurate.
- A full register of all implemented changes shall be maintained, including traces of who ordered, tested and approved the changes.

19. PATCH MANAGEMENT

Patch management is an area of systems management that involves acquiring, testing and installing multiple patches to an administered computer system in order to maintain up-to-date software and often to address security risk.

Patch management tasks include the following:

- Maintaining current knowledge of available patches for all systems
- Determining which patches are appropriate for particular systems
- Ensuring that patches are properly tested before installation
- Documenting patch management procedures

To minimise business disruption as a result of network utilisation, reboots and/or the unnecessary use of system resources as much as possible, only critical and or security related patches are deployed.

Baseline requirements:

- In scope are OS, vendor critical and security updates. Windows and Linux errata security updates shall be published and installed as part of a mandatory patch installation schedule. Non errata security Linux and other vendor updates shall be installed based on known or suspected vulnerabilities that pose a high business risk. Where (technical) limitations prevent the automated deployment of security updates, these updates shall be reviewed and installed based on the identified risk level.
- Servers that are directly or indirectly accessible from the internet (i.e. web server directly accessible or indirectly via the reverse proxy) are considered to have a higher risk level than servers that are not externally accessible and are therefore subjected to a stricter patch schedule. These servers shall be patched at least on a monthly basis.
- Non-internet facing servers are considered to have a lower risk level and shall be patched on a quarterly basis.
- Client systems shall be patched on a monthly basis.
- Reports shall be available to check policy compliance and identify vulnerable systems in a timely manner. Quarterly reports shall be created to ensure the policy is applied and the patch management process is working according to the requirements as outlined in this policy.

20. END OF SUPPORT

As part of the life cycle that every operating system and software goes through there is a point at which vendors do not publish new updates anymore (end-of-support). At this point security updates are no longer released and compatibility issues may arise due to unsupported versions of installed software or compatibility issues.

The discontinuation of security updates and patches can make exposure to a high number of vulnerabilities, as well as compliance violations. Because of this, end-of-life policies to better manage its end-of-life transition shall be established.

The importance of the end-of-support should not be ignored because of the below risks:

Increased operational costs: Keeping the systems online will result in mounting operational expenses, as well as the additional investments to make to keep them secure and stable.

Security risks: Increased exposure can be expected to major vulnerabilities and cybersecurity attacks on the company's computer systems, databases and applications running on end of support systems, potentially increasing risk of data leakages or business disruption as a result of malware infections or attacks.

Non-compliance: Intrum is subject to independent audits therefore outdated software should be a key consideration.

Baseline Requirements

- All products that reach the end of their life cycle and are declared by the vendor as end-of-support shall be replaced and/or upgraded before the announced end-of-support date.

21. MALWARE PROTECTION

The term malware (short for malicious software) is generally applied to a variety of malicious computer programs such viruses, spyware, worms, trojans, rootkits etc., designed with the malicious intent of harming a computer system. These malicious programs can perform several functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission. Generally, a malware can attack multiple parts of a computer system:

- Executable program files
- The file-directory system, which tracks the location of all the computer's files
- Boot and system areas, which are needed to start the computer
- Data files

To protect against malicious software and malicious use of assets, additional security controls should be implemented. Such controls may include, but are not limited to, information security policies and guidelines, restricted access, designated development and test environments, virus detection on servers, desktop and notebooks, virus e-mail attachment scanning, web traffic filtering, system compliance scans, intrusion prevention/detction monitoring and response, logging and alerting on key security events, application whitelisting, information handling procedures based on data type, application and network security testing and system and application vulnerability scanning.

Baseline Requirements

- All workstations, laptops and servers provided shall be equipped with the latest version of an reputated antivirus software. An automatic process shall take care to keep the antivirus program up to date.
- Virus definitions shall be updated immediately after the release by the provider.
- The antivirus software shall be configured to run real-time scanning of machines and a full system scan on a regularly scheduled interval.
- All e-mails entering the mail gateway shall be scanned for suspected payloads. If the payload is definitely suspicious, the mail shall be dropped. If the system is in doubt, the addressed user shall be informed that a mail is placed in quarantine, and given the opportunity to check the contents. The mail gateway appliance shall be constantly and automatically updated with the latest threat definitions.
- An Intrusion Detection System and Intrusion Prevention System shall be used and the logs generated from the system shall be monitored on daily basis.
- On a virus outbreak, an alert shall be generated. The affected workstations shall be identified and affected workstations shall be:
    - Immediately physically disconnected from the network.
    - Manually scanned.
    - If this does not prove to be effective enough, the workstation shall be re-installed.
- In addition to the above controls, internal and external network vulnerability scans shall be run at least on quarterly basis.

22. BACKUP POLICY

The aim of the backup policy is to ensure that data is not lost and can be recovered in the event of an equipment failure, intentional or accidental destruction/loss of data or a disaster. The supplier shall conform to a standard backup and recovery process in such a way that a balance between ensuring legislative compliance and service efficiency is achieved. In addition to that, specific controls shall be enforced so that any risks associated to the management of data backups and recovery are mitigated.

Baseline Requirements

- All production critical systems and data, essential to the continued operation of the supplier, shall be fully backed up at least on daily basis.
- The supplier shall be inform if a scheduled back-up results in consecutive failures.
- When the data in a system changes frequently, backups shall be taken more frequently to ensure that data can be recovered in the event of a system failure.
- Immediate full data backups shall be taken when data is changed to a large extent or the entire database needs to be made available at certain points in time. Regular, as well as event-dependent intervals shall be defined.
- Important data shall be saved by running daily incremental backups and full back-up weekly.
- Entities with specific country requirements on separating tapes from other entities shall be placed in separate retention groups and thus get separate tapes.
- Partial system restores, in the form of ad-hoc restoration of selected file-sets and databases shall be performed regularly as part of the Incident Management process.

- Restoration procedures shall be regularly checked (at least annually) and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
- The supplier shall adhere to data retention requirements to ensure compliance with legal, regulatory and business requirements. No disposal or destruction shall take place without confirming that the data has reached the end of its retention period and that there is no additional retention period (such as a litigation hold or preservation notice) as agreed upon.
- Backup data that is older than 1 month old shall be subject to an approval process before it is released to the requester, to ensure protection of older data that might belong to third parties (e.g. divested companies) or might be related to a data subject that has requested his/her data to be erased.

23. SYSTEM LOGGING AND SECURITY MONITORING

In order to provide a comprehensive security approach against internal and external threats, extensive logging and monitoring of systems and users' activities shall be performed. This policy establishes the minimum practices to implement effective logging and security monitoring of networks and systems to make sure that they are used for authorised purposes only and to detect potential security issues.

Baseline Requirements

- All systems shall, at minimum, be capable of and configured to:
    - Produce audit logs with the necessary event information.
    - Have the ability to off load audit log data to a central syslog server.
- A central log collection system shall be in place in order to collect log data to a single location for log management purposes.
- Logs shall be only accessible by a small set of support personnel. Access to modify or delete log files shall be restricted and segregated so users that perform privileged activities are unable to manipulate log files.
- Security-relevant events shall be logged and monitored to identify suspicious activities and threats. Identified suspicious activities shall be investigated and managed based on their risk and criticality. At minimum, the following information shall be available:
    - Traceability to an individual (data, time, user ID).
    - Successful and unsuccessful login attempts.
    - Highly privileged account activities.
    - Security configuration and setting changes.
- Logs must be retained for a minimum of 12+2 months from time of event or logging, except where prohibited or otherwise required by applicable laws and regulations. Logs relevant to pending or foreseeable litigation, investigation or audit (even when not subject to a formal document retention notice) shall be preserved.
- Identified anomalies shall be registered and processed.
- Personnel shall be informed about the practice of system logging and security monitoring in the privacy statement for personnel.

24. CLOCK SYNCHRONISATION

In computer networks time synchronisation is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events happened. Time also provides the only frame of reference between all devices on the network. Without synchronised time, accurately correlating log files between these devices is difficult, even impossible. Following are just a few specific reasons:

- Tracking security breaches, network usage, or problems affecting a large number of components can be nearly impossible if timestamps in logs are inaccurate. Time is often the critical factor that allows an event on one network node to be mapped to a corresponding event on another
- To reduce confusion in shared filesystems, it is important for the modification times to be consistent, regardless of what machine the filesystems are on

- Billing services and similar applications must know the time accurately
- Financial services require highly accurate timekeeping by law

Baseline Requirements

- The clocks of all information processing systems shall be synchronised with an accurate time source.
- All systems that are able to be configured to use NTP shall use the Domain Controllers as their primary time synchronisation source; if the Domain Controllers cannot be used due to NTP version compatibility issues, an alternative NTP server can be used.
- If possible, for redundancy purposes at least two NTP servers shall be configured on each system.
- The Domain Controllers shall be synchronised with reliable and redundant external NTP servers.

25. VULNERABILITY MANAGEMENT

Vulnerability Management is the process in which vulnerabilities within IT systems are identified, classified and the risks associated to these are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or obtaining a formal risk acceptance by the management of an organisation.
This security process is essential in order to obtain a continuous overview of the vulnerabilities affecting its IT infrastructure and components.
Third party penetration tests shall be conducted at regular intervals, minimum annually and upon all major relevant changes, for all externally facing (available on the internet) applications. Intrum must be given access to reports from such testing, or to a trusted third party statement that the penetration tests have been performed, including a description of the test, the scope of the test and methodology used, who conducted the test and when, in addition to any critical findings.

Baseline Requirements

- An enterprise class vulnerability scanning and assessment tool shall be used to conduct the internal and external scans. This tool must be capable of scanning information systems from a central location and be able to provide remediation suggestions.
- The scans must cover all critical information assets and should be run against all systems on the network at least on a quarterly basis.
- Scans shall be performed during hours appropriate to the business needs and to minimise disruption to normal business functions.
- The vulnerability scanning tool must have the ability to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability
- Vulnerability intelligence services should be subscribed in order to stay aware of emerging exposures, and use the information gained from this subscription to update the vulnerability scanning activities on at least a quarterly basis.
- At the conclusion of each vulnerability scan, all discovered vulnerabilities shall be documented and communicated into a formal report which must also contain the recommended remediation.
- "High" or "Critical" vulnerabilities shall be addressed within 30 days from initial reporting.
- "Medium" vulnerabilities shall be addressed within 90 days from initial reporting.
- "Low" vulnerabilities shall be addressed within 180 days from initial reporting.
- If a system has a vulnerability that cannot be remediated in the recommended manner and within the required resolution time, an IT&IS Risk Assessment shall be performed and the implementation of appropriate security controls to mitigate identified risks shall be proposed.
- Any outcomes from the vulnerability scans shall be treated as confidential.

26. SOFTWARE LICENSING

A software license is a legal instrument allowing the use or redistribution of proprietary software. Without a license agreement, using the software would constitute a breach of copyright law. Therefore any software must be legally licensed before it can be installed.

On top of the legal component, installing unauthorised software on a computer system, workstation, or server can lead to potential system failures, system degradation or viruses. Unauthorised installations also place the business and the employees at risk for civil and criminal action, which can result in punitive measures imposed on all involved parties.

Baseline Requirements

- Installation of software not related with business purposes is strictly forbidden. Users shall be prohibited to install unlicensed and unauthorised software on systems as this may violate copyright protection regulations and/or cause technical problems.
- It is strictly forbidden to use unauthorised registration keys, obtained from anyone or any websites providing illegal serial numbers and registration keys through crackers or Keygen groups.
- Periodic software usage reviews for approved, licensed software shall be performed annually to detect software instances exceeding current license agreements in place.
- Periodic software usage reviews to detect personal, unlicensed software shall be performed every six months.
- Non-compliance shall be reported to Intrum.

27. FIREWALL AND NETWORK SECURITY POLICY

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. While firewalls are often discussed in the context of Internet connectivity, they may also have applicability in other network environments. For example, firewalls may be employed to restrict connectivity to and from the internal networks used to service more sensitive functions, such as accounting or sales. By employing firewalls to control connectivity to these areas, an organisation can prevent unauthorised access to its systems and resources. The implementation of a proper firewall provides an additional layer of security.

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols and applications based on the Intrum information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by Intrum and categorise how they shall be secure including which types of traffic can traverse a firewall under what circumstances. This risk analysis should be based on an evaluation of threats, vulnerabilities and countermeasures in place to mitigate the potential risks. Firewall policy should be updated frequently as classes of new attacks or vulnerabilities arise, or as per Intrum needs regarding network applications change.

The purpose of this policy is to specify the minimal level of security requirements that apply to the network infrastructure. This policy dictates the use of various different types of security controls to reduce risks to both Intrum and its customers based on the sensitivity and business criticality of the respective (data) asset and or network segment. It also explains which eligible entities can connect to the network and the possible restrictions that shall be enforced.

Baseline Requirements

- A tiered network design shall be implemented to isolate systems based on the sensitivity and criticality of the systems or hosted applications.
- Separated network zones shall be defined in order to implement specific network access control rules.
- When traffic is moving from one network zone to another, this shall be classified as passing a security boundary.
- All traffic crossing security boundaries shall be logged and monitored.
- A Demilitarised Zone (DMZ) shall be implemented to limit inbound traffic to only system components that provide authorised publicly accessible services, protocols, and ports.
- If various DMZ networks exist, network traffic between DMZs shall be restricted and monitored
- Externally accessible Web Servers shall be always placed in DMZ. HTTPS shall be always used for secure communications.

- Direct access between the Internet and any internal system component shall be blocked by the firewall systems.
- Inbound and outbound Internet traffic shall be restricted to that which is strictly necessary.
- All firewall rules shall take into account the source and destination of the traffic in addition to the protocol and network ports required. Creation of firewall access rules allowing "ANY" source/destination and "ANY" network protocol/ports shall be limited to the minimum.
- All firewall change requests shall be recorded in an ITSM system. All requests for change shall be assessed in a structured way to determine the security and operational impact to the systems in scope.
- A firewall log retention policy shall be in place. All firewall logs shall be backed up and kept available for at least 2 years.
- Vulnerability assessments shall be performed on regular basis to ensure that the firewall systems are not vulnerable to the latest exploits.
- Firewall systems shall be kept up to date with manufacturer provided firewall software and OS updates and security patches.
- A Firewall housekeeping process shall be established in order to perform a regular review of the configuration, position, and clean-up of the existing firewall rules. Obsolete rules, IPs and protocols/ports that should have been temporary or that are no longer in use shall be removed. The review shall be performed at least on annual basis.
- The progress and findings of each Firewall review shall be documented in a formal document.
- An Internet traffic control solution (URL filtering) shall be implemented. All outbound Internet traffic shall be inspected in order to prevent access to malicious websites.
- An Intrusion Detection System and Intrusion Protection System (IDS/IPS) shall be deployed. All Data Centre and WAN traffic shall be in scope of the system. IDS/IPS signatures shall be updated on daily basis.
- An anti DDoS (Distributed Denial of Service) solution shall be deployed to protect the Internet connection from volumetric and specific application-focused attacks. Functionality tests of the anti DDoS solution shall be performed at least on bi-annual basis.

28. FILE TRANSFER POLICY

Sharing company files or exchanging client's files containing sensitive data via an insecure communication channel, is a major security risk. When it comes to transferring files, keeping sensitive data secure should be a top priority and SFTP and FTPS should be used instead of FTP.

Baseline Requirements

- Outbound and internal file transfers shall be always authenticated and encrypted using secure transfer protocols such FTPS and/or SFTP.
- Files containing confidential information shall be moved and stored at a secure network zone, or encrypted, after they have been processed. File transfer servers exposed on the Internet shall not be used for long-term data storage of unencrypted data.
- Use of cloud-based file transfer services and cloud-based storage solutions (e.g. Dropbox, WeTransfer, Google Drive etc.) is prohibited unless an exception is explicitly granted. The URL filtering policy shall block access to any cloud-based file transfer and storage solutions (note that the policy itself is leading, and an absence of active blocking at the network-level does not constitute permission to use said cloud-based file transfer services).

29. IT SECURITY IN SOFTWARE DEVELOPMENT & SYSTEM IMPLEMENTATION PROJECTS

Investing IT resources (people, applications, facilities and technology) to develop, acquire, integrate and maintain application systems is crucial for the effective functioning of key business processes. These resources, in turn, often control critical information assets and therefore should be effectively managed. IT processes for managing and controlling these IT resources are part of a life cycle process with defined phases commonly known as business application development, deployment, maintenance and retirement. Each phase in the life

cycle is an incremental step that lays the foundation for the next phase, for effective management control in building and operating business application systems.

The software implementation project begins when a feasibility study is initiated as a result of one or more of the following situations:

- A new opportunity that relates to a new or existing business process
- A problem that relates to an existing business process
- A new opportunity that will enable Intrum to take advantage of technology
- A problem with the current technology
- Alignment of business applications with business partner/industry standard systems and respective interfaces

All critical business objectives have to be translated into key business drivers for all parties involved in business operations during a software development project.

Testing is an essential part of the development process that verifies and validates that a program, subsystem or application performs the functions for which it has been designed. Testing also determines whether the units being tested operate without any malfunction or adverse effect on other components of the system.

Developed early in the life cycle and refined until the actual testing phase, test plans identify the specific portions of the system to be tested. Tests plans include a categorisation of types of deficiencies that can be found during the test.

Baseline Requirements

- Group software applications shall be developed within the guidelines of best practices and industry standards.
- Before use of new technology, and before implementing solely automated decision making, a risk assessment including privacy risk assessment shall be conducted by the Technical system owner. If a potential high risk to privacy is identified, a Data Protection Impact Assessment (DPIA) shall be made.
- The OWASP Security Framework and its Secure Coding Practices Checklist shall be used as reference.
- Systems developed must satisfy definite security requirements, including data verification, securing the code before being put in production, and use of encryption.
- Group Information Security shall be involved in the validation of the security requirements.
- Development and system test activities shall not be performed on production environments.
- Production environments shall be either logically or physically separated from development and test environments.
- Where physical separation for development and test is not feasible, security measures for the test environment shall be at least equal to the ones required for the production environment.
- Where possible, development and test data shall be synthetic (fictive) or pseudonymized (masked personal data), not live production data.
- If test data is not pseudonymized, special measures shall be put in place to protect the data. This includes
    - Employee awareness: special trainings, rules and procedures on testing with personal data under GDPR
    - Strongly limit access to the test environment and ensure that production users do not have access unless it is the same person conducting the work in both environments
    - Same logging, log collection and monitoring of use as in production
    - Data amount reduction: e.g. using 5-7% of production database, not 100%
    - Regular audits on test data and testing principles
    - Visualize that testers are in test environment by e.g. different color screens to ensure that they don't confuse production with test
    - Functionality limitation - ensure that all integrations that might impact privacy are disabled or modified in test, such as e.g. the possibility to request credit information about a debtor

should not be available in test, sending an email to a debtor should just go to an internal mail server etc.
    - Same data retention periods as in production / frequent refresh to remove old data
- Logon procedures and passwords shall be different for production, development and test environments.
- Externally accessible Web Servers shall be always placed in DMZ (Demilitarised Zone).
- HTTPS shall be always implemented for secure communications.
- Strong authentication (two-factor-authentication) shall be used to access confidential and restricted data if these are made available through a web interface or API over an open network.
- User authentication for internal Web Services shall always be integrated with Active Directory in order to keep track of logs, improve auditing and inherit account/password security settings.
- User authentication for internet facing Web Services shall always require strong passwords, password expiration periods and account lockout policies, and two-factor authentication shall always be offered. Any user access and key events must be logged and audit log files must be protected against tampering.
- Access to production application, program or object source code and libraries must be based on least privilege principle.
- All systems storing personal data shall support the regular deletion or anonymization of data. If data processing is based on user consent, the systems shall also support the deletion or anonymization of data when the user withdraws his/her consent.
- All systems storing personal data shall enable rectification of personal data that has been identified as wrong. The systems shall also trace the changes being made to personal data, to enable identification of the person changing the data and the time the data was changed.
- Development activities carried out by developers and external consultants should be in line with industry standards and frameworks.
- Developers shall be trained according to recognised good practice and security guidelines.
- Development activities shall include risk mitigation strategies for the common vulnerabilities below:
    - Injection flaws
    - Broken authentication and session management
    - Cross-site scripting
    - Insecure direct object references
    - Security misconfiguration
    - Sensitive data exposure
    - Missing function level access control
    - Cross-site request forgery
    - Using components with known vulnerabilities
    - Invalidated redirects and forwards
- Various levels of testing shall occur during the development phase to verify and validate what has been developed:
    - Unit Testing
    - Interface/Integration Testing
    - System Testing (Recovery Testing, Security Testing, Load Testing, Volume Testing, Stress Testing, Performance Testing)
- During a migration to a new system, a comparison shall be performed between data from the "legacy" system and data loaded to the "new" system. Differences shall be investigated and resolved on a timely basis.
- Errors and irregularities shall be identified from the actual tests conducted. When such problems occur, the specific tests in question have to be redesigned in the test plan until acceptable conditions occur when the tests are redone. The problems should be fixed prior to implementation.
- Quality Assurance Testing shall be performed on all software development projects. QAT verifies that the application works as documented by testing the logical design and technology itself.

- User Acceptance Testing shall be performed on all software development projects. UAT verifies that the system is production-ready and satisfies all documented requirements.
- QAT results shall be formally approved before being transferred to the production environment.
- End users and system administrators shall be trained in how to properly use and maintain a new implementation.
- Post-implementation testing (e.g., parallel processing) shall be performed.
- End-user management shall document lessons learned and/or plans for addressing system deficiencies as well as recommendations for future projects regarding system development and project management processes followed.

30. REMOTE CONTROL SOFTWARE POLICY

Remote Control Software allows authorised individuals to "take control" of a computer across the network from another location. Although this feature would be useful to the local helpdesk teams and in some cases to external suppliers for troubleshooting purposes, it presents several risks which may have a negative impact to the confidentiality, availability and integrity of the systems and information.

Baseline Requirements

- The only allowed software to perform Remote Control of workstations is Microsoft Skype and Bomgar.
- Remote Control Software such as TeamViewer and LogMeIn are not allowed and shall not be installed on any server and/or workstation.

31. CRYPTOGRAPHY POLICY

The primary purpose of encryption is to protect the confidentiality, integrity and availability of digital data stored on computer systems or transmitted via the Internet or other computer networks. Encryption is generally used to:

- Protect data in transit over networks from unauthorised interception and manipulation
- Protect information stored on computers from unauthorised viewing and manipulation
- Deter and detect accidental or intentional alterations of data
- Verify authenticity of a transaction or document

Encryption is limited in that it cannot prevent the loss or modification of data. The protection of the keys is of paramount concern when using encryption systems.

Information system resources shall be appropriately protected to prevent unauthorised access by applying a level of encryption to sensitive and/or critical information which is proportionate to the business risk. The purpose of the below requirements is to protect the confidentiality, integrity and availability of information by applying appropriate levels of cryptographic controls.

Baseline Requirements

- For externally accessible services, secure communication channels based on strong ciphers suites shall always be used (e.g. HTTPS, SSH, SFTP etc.). Use of weak ciphers is prohibited.
- Access to confidential and restricted data or asset is granted only if encryption measures are in place for securing the transactions from outside the office location.
- All confidential and restricted data transferred outside controlled networks shall be encrypted.
- E-mails (including attachments) shall be encrypted whenever confidential and restricted data is contained or attached.
- Unencrypted e-mail and SMS containing personal data can be accepted if the data subject has consented to such transfer
- Unencrypted e-mail and SMS containing personal data within the special categories of data or related to criminal convictions is prohibited even with consent from the data subject
- All laptops shall be protected with harddisk encryption. Information encrypted can only be decrypted by the owner of the master key.

- Full disk encryption should be enabled on all teleworking devices (e.g. mobile phones, tablets, laptops etc.).
- All removable media shall be encrypted.
- Wi-Fi Protected Access encryption is mandatory for all wireless networks carrying information.
- Database encryption is required for all new systems that store personal data

32. SYSTEM HARDENING AND SECURITY REQUIREMENTS

The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner and removing all non-essential software programs and utilities from the computer. While these programs may offer useful features to the user, if they provide "back-door" access to the system, they must be removed to minimise exposure to threats and to mitigate possible risks.

Hardening baseline includes:

- Removal of unnecessary accounts (including service accounts)
- Disabling or removal of unnecessary services
- Applying security patches
- Closing listening and unused network ports

Baseline Requirements

- Unwanted communication channels shall be disabled (i.e. when HTTPS is required disable the use of normal HTTP).
- For DMZ systems (or otherwise publicly accessible systems) secure communication channels based on strong ciphers shall be used (SSH, HTTPS, etc.); use of weak ciphers is prohibited.
- Default configuration of applications and appliances shall be modified (e.g. change default admin passwords).
- Cached credentials shall be disabled for all systems located in the DMZ.
- Remote Root login privileges on DMZ servers shall be disabled.
- Interactive logon for service accounts shall be disabled.
- Individual user accounts shall be always used (authentication based on AD, LDAP, Radius, local user accounts, etc., AD-based authentication is strongly preferred). Access attempts shall be trackable and auditable, with syslog compatibility being strongly preferred. Windows Systems must be domain members (including DMZ servers).
- Local audit logs shall be forwarded to the central syslog server.
- Depending on the function of the system, permissions shall be delegated to the correct people (least privilege principle) and only to data that the user is allowed to access (authorisation based on role or office).
- Unneeded file shares shall be removed and active file shares shall be accessible only to the people that need access to the files to perform their jobs (i.e. no access for the “everyone group”). Hidden shares (Share$) shall be used as much as possible.
- Installed roles and features shall be kept to a minimum and shall be installed only when required by the server for providing the required functionality (i.e. do not install FTP server if only a webserver is required).
- Systems shall be installed with the latest critical and security updates (Windows Updates).
- Systems shall be installed with the latest version of the anti-virus software (Agent and VSE) and have the latest signature files installed.
- Default “public” community string for SNMP access shall not be used.
- Servers/appliances shall synchronise its time from the domain controllers
- Configuration and data (where applicable) backups shall be performed regularly (e.g. export of configuration etc.).

- Physical access to systems shall be limited to authorised personnel only. Performance and availability monitoring shall be in place (SNMP, e-mail notifications from the system etc.).
- When third party support access is required, an NDA must be in place between the entity and the third party.
- Standard configuration management shall be followed, building secure images that are used to build all new systems that are deployed. Regular updates to the secure images should be integrated into the organisation's change management processes. Images should be created for workstations, servers, and other system types used.

33. THIRD PARTY MANAGEMENT

The security of information that are accessed, processed, communicated to or managed by external parties, should be maintained and should not be decreased by the introduction of external party's products or services. Any access to information processing facilities and communication of information by external parties should be controlled. Controls should be agreed to and formally defined in the contract with the external party. Intrum shall gain the right to audit the implementation and operation of the resulting security controls.

These external party arrangements can include:

- Service providers such as Internet Service Providers (ISPs), network providers, telephony services providers, managed security services providers, maintenance and support services providers
- Outsourced facilities and/or operations (e.g., IT systems, data collection services, call center operations, payroll systems)
- Management and business consultants, independent auditors
- Software developers
- Cleaning, catering and outsourced support services
- Temporary personnel, internship, students and other casual short-term appointments

Baseline Requirements

- Access by external parties to information shall not be provided until the risk assessment has been made, the appropriate controls have been implemented and both a Non-Disclosure Agreement (NDA) and a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. It should be ensured that the external party is aware of its obligations and accepts the responsibilities and liabilities involved in accessing, processing, communicating or managing information and information processing facilities.
- Remote Access for third party users shall be limited in accordance with the business requirements and any access connection and operation activity shall be logged. Required access must be explicitly defined and granted by the appropriate manager via a digitally signed form.
- Third parties involved in processing of confidential or restricted data shall be subject to a regular vendor security risk assessment with regular intervals.
- To ensure the return or destruction of confidential information disclosed to a third party, responsibilities shall be in place to manage the process, including the return of all equipment and removal of access rights. The access rights of all contractors and third party users to information and information processing facilities shall be removed within 24 hours upon termination of their contract/agreement. The access rights shall be removed including physical and logical access, keys, identification cards and removal from any documentation that identifies them as a current partner.

34. SECURITY INCIDENT MANAGEMENT

To minimise the impact of any potential security incident and to promptly recover and learn from such incidents, a formal incident response procedure shall be established . Such procedure provides guidance to both technical and managerial staff to enable a quick and efficient recovery from security incidents and to carry out all necessary steps to correctly handle a security incident.

The Security Incident Management process includes the following phases:

- Detection
- Analysis
- Containment
- Remediation
- Resolution
- Incident Closure
- Lessons Learned

Employees and contractors should be aware of procedures for reporting the different types of incidents (e.g., security breach, threat, weakness or malfunction) that might have an impact on the security.

Baseline Requirements

- Information security events and weaknesses shall be reported, immediately after they are seen or experienced, to Intrum.
- All security incidents shall be centrally tracked and reported.

35. AUDIT, MONITORING AND REVIEW

Intrum has the right to perform security related audits, testing and inspections, towards which the supplier shall provide reasonable assistance and documentation in support of the intended outcome of the audit. In regard with such audits, Intrum has the right to engage one or more third party(ies) of its choosing to assist in the execution of security related audits, testing and inspections, or execute them on Intrum's behalf.

Such security audits, tests and inspections shall for the avoidance of doubt be confined to areas, systems and infrastructure which could conceivably impact the security of Intrum, the data or the supplier's ability to fulfil its obligations.

Security audits, tests and inspections shall be limited to once per 12 months, unless:

a) a security audit, test or inspection conducted during the preceding 12 months has identified severe findings (e.g. severe weaknesses, vulnerabilities or deficiencies, of a technical or organisational nature), which shall be reasonable grounds for a follow-up audit or audit of an expanded related scope
b) a severe security incident materially impacting Intrum, data or the supplier's ability to fulfil its obligations, has occurred or can reasonably be suspected, which shall be reasonable grounds for audit of the related technological and organisational scope
c) a breach of security regulations agreed between Intrum and the supplier has occurred or can reasonably be suspected, which shall be reasonable grounds for audit of the related technological and organisational scope, or
d) a change has occurred which could reasonably be assumed to impact the security or stability of the deliverables, or that of Intrum assets depending on said deliverables.

Unless negatively impacting the purpose or outcome of the security audit, test and/or inspection in question, Intrum shall provide no less than two weeks advance notice of such security audits, tests and inspections. Advance notice of no less than 24 hours shall nevertheless be provided in all instances. In addition to the said obligations, Intrum has the right to conduct security testing prior to taking the deliverables into first use, and the supplier shall reasonably accommodate for Intrum's activities in its project planning.

The supplier shall allow Intrum to perform regularly monitoring of compliance with applicable laws and verify contractual control effectiveness. The supplier shall perform a compliance review or a self-assessment yearly relating to information security requirements. If any non-compliance is found as a result of the review, the supplier shall evaluate the need for corrective actions and document the result.

The supplier shall present audit/assurance reports to Intrum. The supplier will respond to the recommendations of the report, develop a remediation plan and carry out the remediating actions required to achieve a satisfactory resolution of the respective control deficiency.

Sikkerhetsforanstaltninger, inkludert retningslinjer for oppførsel og sertifiseringer.