conexus
FRIGJØR KUNNSKAP

I henhold til personopplysningslovens § 13, jf. § 15 og personopplysningsforskriftens kapittel 2.

mellom

Askim kommune
Org nr 840894312
Behandlingsansvarlig

og

Conexus Norge AS
Org nr 996 014 436
Databehandler

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften). Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlers bruk av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

2. Formål

CX Stafettloggen er et system for bedre tverrfaglig samhandling på tvers av offentlige hjelpetjenester som er ansvarlig for barn og unge med behov for bistand.
Systemet er bygd for å sikre fokus på innsats for å bedre eller fjerne barnets registrerte utfordring gjennom tverrfaglig samhandling mellom de offentlige hjelpetjenestene, barnet og barnets foresatte.

Formålet med registrering og behandling av data i CX Stafettloggen er å sikre kommunikasjon, koordinasjon og samarbeid i arbeidet med enkelt individets utfordring. Dataene registreres i CX Stafettloggen og bearbeides av vedkommende som har rolle som Stafettholder. Registrering av data i løsningen er forutsatt av foresattes informerte samtykke for registrering av data og utveksling av informasjon mellom spesifikke aktører.

Personopplysningene som skal behandles er definert i vedlegg 1.
Dataene skal behandles som sensitiv informasjon og rammene for behandling er gitt av:

- Vedlegg 2 definisjon av sletteprosedyrer
- Vedlegg 3 Tilgang og lokasjon til produksjonsdata
- Vedlegg 4 Prosedyre for behandling av produksjonsdata.

3. Databehandlers plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtale eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

4. Bruk av underleverandør

Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avtales skriftlig med behandlingsansvarlige før behandlingen av personopplysninger starter.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

Vedlegg 3 beskriver utnyttelsen av underleverandører og deres tilgang til produksjonsdata.

5. Sikkerhet
Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven og personopplysningsforskriften, herunder særlig personopplysningslovens §§ 13 – 15 med forskrifter. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at databehandler melder avviket til behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

6. Sikkerhetsrevisjoner
Behandlingsansvarlig skal avtale med databehandler at det gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne avtalen.

7. Avtalens varighet
Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

Ved brudd på denne avtale eller personopplysningsloven kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Avtalen kan sies opp av begge parter med en gjensidig frist på 12mnd, jf. punkt 8 i denne avtalen.

8. Ved opphør
Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av denne avtalen.

Det skal avtales at databehandler skal slette eller forsvarlig destruere alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Avtalen bør spesifisere på hvilken måte sletting og/eller destruksjon skal skje etter avtalens opphør.

Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Videre kan det avtales at det skal gis en utskrift og kopi av alt innhold i databaser og lignende med data som er omfattet. Kostnader ved dette skal inngå i en slik avtale.

9. Meddelelser
Meddelelser etter denne avtalen skal sendes skriftlig til: support@conexus.no

10. Lovvalg og verneting
Avtalen er underlagt norsk rett og partene vedtar Drammen tingrett som verneting. Dette gjelder også etter opphør av avtalen.

Databehandleravtalen har fire vedlegg

***

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Sted og dato
Drammen 2/3-16

Behandlingsansvarlig	Databehandler
(underskrift)	(underskrift)

PERSONDATA & ANONYMISERING

I CX Stafettloggen vil det kunne registreres persondata for rollene som barn/elev, foresatte, stafettholdere og aktører i det tverrfaglige nettverket i kommunen.

I CX Stafettloggen vil det registreres følgende type persondata:

- Samtykke innhentet
- Barn/Elevers navn, fødselsnummer, bostedsforhold
- Foresattes navn, fødselsnummer, telefonnummer, epostadresse
- Vurdering av omfang på barnets behov for bistand via en 3-trinns skala
- En vurdering av barnets utfordringer gjennom predefinerte kategorier og et begrenset fritekstfelt
- Konkretisering av mål for utvikling via et begrenset fritekstfelt
- Konkretisering og evaluering av tiltak via predefinerte kategorier og et begrenset fritekstfelt
- Konkretisering av hvem som er ansvarlige for gjennomføring av tiltak
- Konkretisering av tidsfrister, møtetidspunkter, og hvorvidt det har foregått drøftinger med leder og foresatte rundt barnets utfordringer.

Når formålet med behandling av informasjonen opphører, eller samtykke trekkes vil informasjon om oppmerksomhet og tiltak, med unntak av eventuell benyttede fritekstfelt bli lagret med knytning til virksomhet og kommune.

For å sikre total anonymitet er det implementert prikkeregler som fjerner visualisering av informasjon dersom antallet registreringer sannsynliggjør en indirekte identifikasjon. Formålet med ivaretakelsen av disse data er å sikre informasjon for skalering og evaluering av iverksatte tiltak i den hensikt å forbedre kommunens evne til å levere tjenester til gode for fremtidige barn med behov for tverrfaglig innsats.

De spesifikke data som blir bevart per kommune er:

- Oppmerksomhet assosiert til kommune og virksomhet
    - Valgt kategori i forhåndsdefinertliste
    - Valgt kategori for alvorlighetsnivå på oppmerksomhet
    - Dato for oppmerksomhet
    - Stafettholder
- Tiltak assosiert til oppmerksomhet
    - Valgt kategori i forhåndsdefinertliste
    - Datofelter for tiltak
    - Aktører
    - Vurdering av tiltak basert på valgt kategori i forhåndsdefinertliste

De implementerte prikkereglene er som følger:

1. Resultatene på filtreringer hvor det er færre enn 5 registreringer, skal skjermes (prikkes).
2. Når kategori fordelingen er vist, skal alternativene skjermes hvis det kun er ett eller to svar. Er det bare ett alternativ som prikkes ut fra denne regelen, skal også alternativet med den nest laveste svarverdien prikkes (selv om det er 3 eller flere som har valgt dette alternativet).

Information Elements contained within Solution

Type information	Description	Information elements
Actors	Actors that are involved with the child	Name, type of actor
Relationships	Relationships between kid and parents/legal guardians	Role, relationship type
Summaries	Meeting between actors/parents/child	Meeting summary/notes
Child	Information about the child	Name, SSN, Contact information
Actions	Description of actions perform by actors supporting the child	Type of action, description of problem, diagnosis
Notes	Notes from actors supporting the child	Free text
Resources	Information resources that can be used by actors to help child	Links to publicly available information

INFORMATION DELETION LOGIC

When is data deleted
Roles in the system:

- Municipality administrator
- Organisational Manager
- Relayholder
- Actor
- Guardian/Parent
- Child

	Scenario	Action	Data in Production	Accessibility to production data by system users.	Data in Backup
1	The child becomes of legal age	The individual Child is flagged in administration interface. Municipality administrator needs to execute on the flagged child by producing a report for potential archiving and set deletion of record in administration interface. Upon completion of report procedure and the option of deletion of record is set, all personal identifications are deleted from the database(s) and removed from the results.	Upon execution of the described action for system administrator the identification is automatically removed within 24 hours and data linked to the individual is only available in the report if produced. The report is maintained accessible in the system for 12 months.	Municipality administrator	All result records with personal identity are maintained unchanged in backup for 30 days. The report is maintained in backup for a total of 12 months + 30 days.

	Scenario	Action	Data in Production	Accessibility to production data by system users.	Data in Backup
		The results are kept for statistical purpose. The statistics will increase the ability to execute the most efficient actions towards the child(ren).			
2	The child becomes of legal age and request data to be deleted.	The scenario is identical to that of 1) with the exemption that the system administrator needs to effectuate the procedure in a more time stringent manner.	Equal scenario 1)	Municipality administrator	Equal scenario 1)
3	The guardian requests data to be deleted	The logg is set passive and transferred to Organisational manager for potential archiving and deletion according to the procedure of the municipality. No further recording of results are allowed.	Data is available and maintained accessible for Organisational Manager and Municipality Manager	Municipality administrator Organisational Manager Relayholder Actors Guardians Child (if given by Relayholder)	No actions is performed.
4	The child changes municipality (juridical region)	see scenario 8)	Data is available and maintained		No actions is performed.
5	There is no activity on the log.	Relay holder receives request after 3 months of inactivity to initiate new meeting or set the log passive.	If set passive: data is available and maintained, but viable only for organisational manager and the municipality administrator.	Municipality administrator Organisational manager	No actions is performed.

	Scenario	Action	Data in Production	Accessibility to production data by system users.	Data in Backup
		If set passive, the log is transferred to Organisational manager to produce report for potential archiving.			
6	The child has a passive logg	The logg is maintained by the Organisational manager to produce report for potential archiving and deletion according to the procedure of the organisation and municipality.	Available in the system for the Organisational manager and the Municipality administrator.	Municipality administrator Organisational manager	No actions is performed.
7	The integrity of the data has been breeched.	Upon indication of integrity breech by either party in the service, communication between product manager and system administrator must be established to identify the extent and root cause of the integrity breech. In-case of or reason to believe external cause (eg. data intruders), the service should be taken down without delay and establish emergency teams to first: - secure excisting data, - correct incorrect information elements and/or remove corrupted data. - reestablish integrity of the system	The service is offline until integrity is reestablished.	non	backup is potentially used for roll-back.

	Scenario	Action	Data in Production	Accessibility to production data by system users.	Data in Backup
8	The child alters organisation and/or Municipality, with consent from guardian(s) to make data from declarant organisation and/or municipality available for recipient organisation and/or municipality.	Handshake protocol between organisations are maintained in the system to ensure consent to transfer is in place. Declarant Organisational manager to produce report for potential archiving.	The logg of activities within the declarant organisation is maintained in the system and available for the declarant organisation. Historical data are made available for recipient organisation. No changes to historical data are allowed.	Municipality administrator Organisational Manager Relayholder Actors Guardians Child (if given by Relayholder)	No actions is performed.
9	The child alters organisation, but consent from legal guardian(s) to make data from declarant organisation available for recipient organisation does not exist.	Declarant organisation receives request after 3 months of inactivity to set the logg passive. See scenario 5)	Data is available within declarant organisation	Municipality administrator Organisational Manager	Data is maintained
10	Organisation discovers the existence of passive logg in other organisation.	Requests declarant organisation to collect consent for transfer of data. Upon consent achieved: see scenario 8)	Data is available and maintained within declarant organisation. If consent is given see scenario 9.	Municipality administrator Organisational Manager If consent is given: see scenario 9	Data is maintained

	Scenario	Action	Data in Production	Accessibility to production data by system users.	Data in Backup
11	Consent from legal guardian(s) has become invalid.	The logg is set passive and transferred to Organisational manager for potential archiving and deletion according to the procedure of the municipality. No further recording of results are allowed.	Data is available for organisation within CX Stafettloggen until deletion procedure is executed.	Municipality administrator Organisational Manager	Data is maintained
12	Consent from guardian(s) is denied.	The logg is never created.	No data exists	non	No data exists
13	Relayholder requests data to be deleted.	Based on subjective and case specific considerations the Relayholder may request a logg to be deleted. The request is performed through making the logg passive and then through a manuall procedure, established at the municipality, provide arguments for deletion of the record with support from the organisational manager. The deletion of record is performed by the Municipality administrator through same procedure as scenario 1.	Equal scenario 1)	Equal scenario 1)	Equal scenario 1)

	Scenario	Action	Data in Production	Accessibility to production data by system users.	Data in Backup
14	Change of actor Change of Relayholder Change of Organisational Manager Change of Guardians	All data registered by the former actor and the identification of the former actor related to a specific registered activity will be maintained in the logg as long as the logg itself is not deleted. The rights of the former actor will be deleted. Updated records of actors associated to the Municipality are the responsibility of the municipality. Same rules apply for the following roles: realyholder, Organisational manager, Guardians.	No change to excisting data	Municipality administrator Organisational Manager Relayholder Actors Guardians Child (if given by Relayholder)	Data is maintained

VEDLEGG 3 - SUB-CONTRACTORS, LOCALIZATION AND ACCESS TO PRODUCTION DATA

Sub-contractors

Name	Org. nr.	Addresse	Purpose	Contact information
Conexus Technology AS	995 807 564	Grønland 67, 3045 Drammen	Provides: Customer Support, Life cycle management and development of solution.	support@conexus.no
Basefarm AS	982 211 743	Nydalen Allé 37A, 0484 Oslo, Norge.	Provides: Physical hosting and server management of production and staging facilities.	post@basefarm.no

Physical localization of production-data

Def: Production data: Data produced through real-life usage containing information about real-life individuals.

Location	Purpose	Environment	Notes
Norway - Basefarm	Production and backup	COE: Production and Staging	
Norway - Conexus Technology AS	Development and test	Cx: Dev & Test	Anonymous data

Access to production data

Changes in personnel requires logging of period and hence incorporation of a new record to identify the new personnel.

Role	Association	Rights
Product Owner-Technical	Conexus Norge	given read - rights
System Owner	Conexus Technology	given read - rights
Solution Architect	Conexus Technology	given read - rights
Operation Manager	Conexus Technology	Managing access rights Maintains read and write rights
Customer Support Consultant	Conexus Technology	No default rights, only when given access by Operation Manager based on justified and documented reason.
Hosting operator	*Basefarm:* (Org. nr. 982 211 743), Nydalen Allé 37A, 0484 Oslo, Norge.	ISO certified with continuous identification log of all activity

Identified personnel per 01.09.2015. Updated lists are given on request.

Role	Name	Date period 1
Product Owner- Technical	Stian Jonson	01.09.2015 - ongoing
System Owner	Geir Fuhre Pettersen	01.09.2015 - ongoing
Solution Architect	Morten Udnæs	01.09.2015 - ongoing
Operation Manager	Olaf Dietzler	01.09.2015 - ongoing
Customer Support Consultant	Christopher Foss	01.09.2015 - ongoing
Hosting operator	upon request to Basefarm	01.09.2015 - ongoing

VEDLEGG 4 - PROCEDURE FOR TREATING (MANAGING) SENSITIVE DATA

The safeguarding of Personal Identifiable Information or Sensitive Personal Information (PII / SPI) is a cornerstone of all management, handling and access of such information. Outmost care must be excercised when doing so.
Not only is this reqiured by Norwegian and international laws, but it is also in the interest of Conexus to protect our operations, assets, and reputation and our obligations concerning information privacy laws, contracts, etc.. The instructions below are provided to avoid data leakage or data loss events. Data leakage or loss events must be handled as per below instructions.
Our systems contain typically 3 different kinds of information according to the following security classification

Security Classifications
Categories of information based upon intended use and expected impact if disclosed. Data classifications are defined by law, but may be classified higher than required by law by data owners.

Data can change its originally defined classification by combining it with other data, which changes the complete data set into either records Personal Identifiable Information or even into Sensitive Personal Information.

If you cannot identify which security classification is the correct one for data you are managing you must always assume that it falls into the category Sensitive Personal Information.

- Public
  Information intended for public use that, when used as intended, would have little to no adverse effect on the individual whos data is processed, Conexus operations, assets, and reputation and our obligations concerning information privacy laws, contracts, etc.. Information typically found on the Internet.
- Personal Identifiable Information
  Personal Identifiable Information is defined as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace or "reasonably ascertainable" an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information
- Sensitive Personal Information
  Sensitive Personal Information is defined as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace or"reasonably ascertainable"an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, which contains information relating to the individualsracial or ethnic origin, political opinions, philosophical or religious beliefs,the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, the individualshealth, his / her sex life, or trade-union membership.

Creation & Maintenance
Records are created as part of the normal course of providing systems and services to our customers. These records document the decisions and activities of our customers and their processes. It is essential that they are only created and maintained appropriately throughout their entire life cycle. Data manipulation for other purposes or through other means than the predefined tools and mechanisms is strictly forbidden.
Sensitive information contained in our systems constitute an area of critical concern because of the severe risk to our customers and Conexus in terms of legal obligations, operations, assets, and reputation, should records be mishandled or information inappropriately accessed or disclosed. As a consequence, records containing sensitive information should exist only in areas where there is a legitimate and justifiable business need.

Sensitive Identifiable Information life cycle must be controlled by way of records retention schedules (prepared in collaboration with customers) and in accordance with Norwegian law. Records schedules will document the existence of these materials, the rationale behind keeping them, and help ensure their availability during the period in which they are vital as either active administrative or historical records. Record retention schedules also will work to ensure the timely disposal of non-permanent, inactive records, thereby mitigating the risk of exposure of information when it no longer serves an active administrative or historical function.

Access
Sensitive Personal Information and Personal Identifiable Information requires strict control, very limited access and disclosure, and may be subject to legal restrictions. In some cases, information is sensitive because it has been aggregated into a single record or document.

Only Conexus employees or members of staff of a data processor,who have authorization from the data owner(s), and have a signed confidentiality agreement on file, may have access to sensitive information.

Any other disclosure of sensitive information requires the written approval of the data ownwer(s) or the appropriate Security Officer of Conexus, in consultation with general counsel as necessary.

Employees are not allowed to take sensitive data off systems, databases or any other type of copy other than required for the execution of their defined duties.
Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform defined duties.

Individuals with access to PII / SPI must respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the responsible management staff at Conexus or the relevant data processor.

A record of all individuals having access to Sensitive Personal Information, databases and systems is to be maintained at all times.

Use and Disposal
The following controls are **required** when using or disposing of sensitive information.
Do not discuss or display Personal Sensitive Information in an environment where it may be viewed or overheard by unauthorized individuals

- Safeguard, access keys, usernames and passwords.
- Do not store usernames, passwords or copies of data in areas, systems or files accessible to unauthorized personnel.
- DO NOT print, (photo)copy or fax it.
- Ensure that any physical output (print, screenshots, etc) are only viewable for authorized personnel.
- DO NOT store any physical output (print outs, screenshots, or data files) outside physical or logical secure locations, which are approved by the Conexus Security Officer.
- Properly identify such information as sensitive to all staff that have access to it. Label it "Sensitive" and provide training and instruction to personnel, accessing or managing the data. Be explicit in instructions and routines on how to manage the information.
- All Sensitve data, stored in electronic systems, must be stored encrypted at a level defined by the Data Owner and/or the Conexus Security officer.
- All encryption keys must be stored and handled under the "Two-Person Concept"
- Follow an established and documented software development lifecycle when building applications that process sensitive information.
- All staff managers are responsible for educating and training employees as to the purpose of this policy and how to excercise the use and disposal of SPI properly.
- Disposal and deletion of physical or electronic records (databases incl. backups, hard copies, computer systems and storage devices) must be automatically recorded or witnessed under the "Two-Person Concept".
- Destruction of electronic instances of PSI by physical destruction or by using a "Nasjonal Sikkerhetsmyndighet" (NSM, norwegian national Security Authority) approved wiping method. **Reformatting a hard drive is not sufficient to securely remove all data.**
- Shred (crosscut shredding recommended) or pulp all highly sensitive information in paper form. This includes all transitory work products (e.g., unused copies, drafts, notes).

Ensure that obsolete computers and electronic media (anything that can store data such as CDs, DVD, thumb drives, diskettes, iPods, etc.) are disposed of properly to ensure that no data remains. This may entail physical destruction of the computer's hard drive (or electronic media) or may instead entail electronic measures such as erasing the hard drive via a "Nasjonal Sikkerhetsmyndighet" (NSM, norwegian national Security Authority) approved method.

Transmission & Transport

The following controls are **required** when transmitting or transporting Sensitive Personal Information:

When sending PSI by mail (including National / International Postal Services, DHL, UPS, FedEx, etc.), the sender must obtain secure, certified, tracking and signature confirmation services and use a tamper-evident sealed package.

The requirement for or encryption of the sensitive data items themselves still applies.

DO NOT place PSI on removable media, or mobile computer systems ((e.g., laptops, PDAs, smart phones); or transmit PSI electronically without the prior approval of the Conexus Security Officer.

If PSI is to be transferred electronically between its original secure data storage and other electronic systems, the transfer must happen through secure, encrypted (minimum standard AES256) channels.

The use of e-mail (also internally within Conexus), instant message, chat or unsecured file transfer (such as FTP) is prohibited, unless the data itself is encrypted at minimum AES256 encryption level.

Do not remove sensitive information from an approved secure location without prior approval of the data owner or the Conexus Security Officer.

In the event that an individual employee or job responsibility requires sensitive information to be removed from the from its original secure data storage, the information (whether electronic or any other form) must be protected at all times from inappropriate disclosure. Appropriate procedures for the protection of the PSI must be in place while outside its original secure data storage. When the data is no longer required to be kept outside its original secure data storage it must be destroyed in accordance with the instruction above.

Any backup copies (Tape, disk, online backup, etc.) of the SPI must be encrypted using an approved encryption method before being sent offsite. Where feasible, alternatives to mail delivery must be utilized such as a secured, encrypted online transmission.

These transmissions that utilize passwords to encrypt or decrypt data must have their own unique identifier or password.

Security breaches and data leakage
If any of the above procedures are breached, the Security Incident Management Process must be invoked and we must assume that a data leakage of Sensitive Personal Information has occurred. (Data Leakage: The unauthorized transfer of classified information from a computer system or datacenter to the outside world. Data leakage can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding)

Access / Analysis
When there is suspicion of a possible data leakage, first assess if a spill has actually occurred, the sensitivity of a potential compromise, the users, time lines (date / time of breach, date / time of discovery), systems, and applications involved.
Analysis is performed to identify the technical details, root cause, systemic problems, and potential impact(s) of a security incident.

Gather all information relevant to the incident (e.g., previously acquired data, event logs, audit trails, and all-source intelligence).

Coordinate with other organizations to gather additional information.
Perform analysis to determine the validity of the incident, identify delivery vectors and system weaknesses, and determine root cause(s) and impact.

Report
Report the suspected incident immediately to the Information Owner (Conexus Security Officer), including the above information.

A report should include a detailed description of the nature of the infringement, which information has (possibly) been lost and what is being done to solve the problems and to mitigate the damage. Furthermore, reference should be made to a contact person and what measures the parties involved can take to restrict their losses.

Use a system to maintain records of security incidents and to safeguard incident data.
Provide updates if there are changes in the incident status.

Isolate

Isolate and contain to minimize damage and preserve evidence that may be required for damage and risk assessment, law enforcement, or counterintelligence purposes. Identify all information hardware and software systems and applications affected, and execute approved procedures to ensure that spilled data does not propagate further. Affected media/devices take on the classification level of the compromised data until response team personnel have assessed the situation and executed appropriate procedures. If classified information appears in the public media, do not make any statement confirming the accuracy or classified status of the information, or discuss it with anyone without an appropriate security clearance and need-to-know. It is possible that verification of a compromise and the resulting damage assessment may result in a classification downgrade of all or part of the data.

Contain
Research and identify incident response actions.

Conexus Security Organization