Барања за информативна безбедност за Снабдувачите (Изведувачите) на Купувачот

Верзија 3.0

Класификација на информации на Купувачот: јавна

Безбедноста на снабдувањето и безбедните услуги се клучни елементи на корпоративната стратегија на Купувачот. Соработката со нашите даватели на услуги (service providers) и Снабдувачи (Изведувачи) е од суштинско значење за успешно спроведување на барањата на информативната безбедност. За нас е важно да ги заштитиме податоците, системите и апликациите со безбедносни мерки во согласност со водечките индустриски стандарди, како што се очекува од една од водечките меѓународни групи во енергетскиот и еколошкиот сектор. Управувањето со односите со Снабдувачите (Изведувачите) во однос на безбедноста е важен дел од нашето внатрешно управување со ризик, вообичаена практика според меѓународните стандарди (на пр., серијата ISO 27000), а исто така може да претставува законски услов за компаниите во критична инфраструктура или како даватели на основни услуги.

Понудувачот, обработувачот, Снабдувачот (Изведувачот) (Contractor), или договорната страна (во натамошниот текст: „Снабдувач (Изведувач)“) на Купувачот претставува и гарантира дека ги исполнила сите потребни обврски за детална ревизија (due diligence), ги познава и ги признава овие безбедносни барања и се согласува да ги почитува кога:

(a) пристапува до објектите, мрежите и/или информациските системи на Купувачот; или

(b) пристапува, обработува или складира информации/податоци на Купувачот; или

(c) обезбедува услуги за ИТ-инфраструктура и/или стандарден софтвер или развива софтвер.

Секое повикување на „Клиент“, во овој документ, се однесува не само на податоците на Купувачот (или системи, услуги итн.), туку и на податоците на клиентите и партнерите на Купувачот. Дополнителни барања за информативната безбедност може да се наведат во поединечни договори (на пр.: SLA, каталог на барања). Овие безбедносни барања ги дополнуваат одредбите за доверливост и безбедност во Општите услови за набавка на Купувачот. Индивидуалните договори помеѓу Снабдувачот (Изведувачот) и Купувачот кои целосно или делумно го заменуваат или дополнуваат овој Договор ќе имаат предност пред овој Договор.

Содржина

1 Управување (Governance)

1.1 Насоки

Снабдувачот (Изведувачот) управува со систем за управување со безбедноста на информациите кој е предмет на континуиран процес на подобрување врз основа на признати стандарди.

Политиките за безбедност на информациите, процедурите, улогите, одговорностите (accountabilities) се пропишани во согласност со деловните барања на Снабдувачот (Изведувачот), релевантните закони, регулативи и заедничките безбедносни стандарди. Политиките за безбедност на информациите се одобрени од раководството, објавени и доставени до вработените и релевантните надворешни страни.

Снабдувачот (Изведувачот) се согласува редовно да ја проверува неговата усогласеност со воспоставените политики и стандарди за безбедност на информациите и сите други барања за безбедност на информациите.

1.2 Управување со ризикот (Risk Management)

Снабдувачот (Изведувачот) има имплементирано програма за управување со ризици за информативната безбедност.

Снабдувачот (Изведувачот) гарантира дека се проценети ризиците кои имаат директно или индиректно влијание врз услугите и/или податоците на Клиентот и дека се преземаат и документираат мерки за намалување на ризикот. Ризиците кои директно или индиректно влијаат врз Клиентот, на барање на Клиентот мора да се пријават.

1.3 Класификација на информации

Бидејќи сите информации немаат иста чувствителност, информациите мора да се класифицираат во степени на доверливост. Доколку Клиентот му даде на Снабдувачот (Изведувачот) информации, тие ќе бидат класифицирани на следниот начин.

Класификацијата е во 4 класи, кои регулираат како треба да се постапува со соодветните информации. Кодирањето во боја се заснова на меѓународниот протокол TLP.

Класа на доверливост	**Кодирање (по боја)**
јавна (public)	бела
интерна (internal)	зелена
доверлива (confidential)	портокалова
строго доверлива (strictly confidential)	црвена

1.4 Договори и спогодби

Снабдувачот (Изведувачот) се согласува да ја вклучи одговорноста за информативната безбедност во договорите со своите вработени и изведувачи.

1.5 Заднински проверки (Background Checks)

Заднинските проверки на кандидатите за вработување од страна на Снабдувачот (Изведувачот) се спроведуваат во согласност со важечките закони и прописи. Обемот на таквите проверки мора да биде пропорционален на ризикот поврзан со улогата на кандидатот.

1.6 Програма за подигање на свеста

Сите вработени на Снабдувачот (Изведувачот) и, онаму каде што е релевантно, изведувачите, се подложени на мерки за подигање на свеста и обука соодветни на нивната улога. Покрај тоа, вработените се информирани и за ажурирањата на политиките и процедурите на Снабдувачот (Изведувачот). Сите вработени мора да ги имаат потребните вештини за нивните улоги и одговорности.

2 Управување со промени

2.1 Животен циклус на информациски средства (Asset lifecycle)

Снабдувачот (Изведувачот) обезбедува безбедноста на информациите да биде составен дел на информациските системи во текот на нивниот животен циклус (стекнување до деактивирање и отстранување на опремата и системите). Снабдувачот (Изведувачот) гарантира дека обезбедените компоненти и нивните оперативни системи, middleware (на пр. Java) и апликациите се поддржани и ги добиваат најновите безбедносни ажурирања. Снабдувачот (Изведувачот) обезбедува редовни безбедносни ажурирања навремено во текот на периодот на договорот.

По раскинувањето на договорниот однос, Снабдувачот (Изведувачот) обезбедува враќање на компонентите (на пр.: уреди, медиуми) доставени до клиентот.

2.2 Управување со промени во софтвер

Снабдувачот (Изведувачот) има имплементирано формални политики во врска со управувањето со промените и безбеден развој на софтвер, кои исто така дефинираат и проверки поврзани со безбедноста. Ревизиите на сајбер (cyber) безбедноста на новите дизајни или системски промени, како и тестирање на безбедноста пред нивната имплементација мора да бидат дел од процесите. Пред да бидат пуштени во употреба, промените се соодветно побарани, авторизирани, тестирани и одобрени.

2.3 Безбеден развој на софтвер

Снабдувачот (Изведувачот) вклучува аспекти од информативната безбедност во својата документација за производи. Таквата документација мора да содржи упатства за конфигурација на услугата и/или околината за да се обезбеди безбедно работење. Развиениот софтвер мора да се тестира во контролирана околина со цел да се детектираат недостатоците пред да се стави на располагање на Клиентот.

Снабдувачот (Изведувачот) гарантира дека животниот циклус на развиениот софтвер содржи соодветни безбедносни мерки (Secure Software Development Lifecycle). Тие вклучуваат, но не се ограничени на:

- користење меѓународно признати методи за безбеден развој на софтвер (вклучувајќи Agile процеси, како што се Scrum, Kanban, итн.) како интегрални елементи на безбеден процес за развој на софтвер;
- безбедни упатства за кодирање засновани на меѓународни стандарди;
- обезбедување интегритет на изворниот код;
- редовни прегледи и проверка на безбедноста на кодовите (статички и динамични тестови на безбедноста на апликацијата);
- скенирање за повреди што вклучува користење код од трета страна и компоненти со отворен код (open-source) (на пр. библиотеки);
- тестови за безбедноста и пенетрациски тестови извршени од независна трета страна;
- соодветна обука за внатрешни и надворешни развивачи на софтвер;
- Детектираните и познати повреди се елиминираат пред да се пушти софтверот во употреба.

3 Доделување на услугата / работата на надворешен Снабдувач (Изведувач) (Outsourcing)

3.1 Предавање на услугата / работата на надворешен подиспорачувач/ подизведувач (Sub-Outsourcing)

Снабдувачот (Изведувачот) има јасни договори со сите подизведувачи на услуги со цел да ја утврди нивната одговорност за безбедноста на податоците на Клиентот што тие ги обработуваат/чуваат/пренесуваат во име на Клиентот. Снабдувачот (Изведувачот) гарантира дека безбедносните мерки што ги спроведуваат подизведувачите се совпаѓаат или го надминуваат нивото наведено во главниот договор. Снабдувачот (Изведувачот), како дел од процесот на управување со Снабдувачот (Изведувачот), ја потврдува ефективноста на овие мерки.

4 Безбедна работа на системот

4.1 Управување со идентитет и пристап

Снабдувачот (Изведувачот) има имплементирано контроли за пристап за да ги потврди идентитетите и да го ограничи пристапот за овластените корисници. Правата за пристап се засноваат на принципот на минимален пристап и на неопходност од пристап базиран на функции. Дополнително, се почитува принципот на „поделба на должностите".

Снабдувачот (Изведувачот) има имплементирано механизми за автентикација според најдобра практика за да го заштити пристапот до системот, кои вклучуваат, но не се ограничени на:

- политика за лозинки (минимум 12 знаци, сложеност, без повторна употреба);
- единствена идентификација на корисникот (избегнувајте генерички и заеднички корисници);
- безбедно складирање/управување/пренос на лозинките

Снабдувачот (Изведувачот) обезбедува заштита на корисничките сметки до кои може да се пристапи преку Интернет со сигурни и силни механизми за автентикација, во најмала рака повеќефакторска автентикација.

Снабдувачот (Изведувачот) има имплементирано строги контроли за привилегираните кориснички сметки (на пр., сметки за системски администратори) преку силни барања за автентикација (на пр., повеќефакторска автентикација), ограничување на минимум и внимателно следена употреба.

Снабдувачот (Изведувачот) ги прегледува правата за пристап на вработените во редовни интервали и ги менува (т.е. ги ограничува/одзема) доколку е потребно. Снабдувачот (Изведувачот) го известува Клиентот за прекин/престанок на работниот однос на вработените кои имаат права на пристап. Сите средства за пристап (на пр. клучеви, картички за пристап, токени за далечински пристап) треба да му се вратат на Клиентот во најбрз можен рок.

4.2 Управување со „закрпи" (Patch Management)

Снабдувачот (Изведувачот) врши редовни анализи на системот (оперативни системи, апликации, мрежни компоненти) за познати повреди. Закрпите (patch) се применуваат на конзистентен и стандардизиран начин, со приоритетност според нивната критичност. Ако коренот на повредите не може да се отстрани во разумен временски период, мора да се преземат алтернативни мерки за ублажување на ризикот додека не се постигне отстранување. Снабдувачот (Изведувачот) има спроведено процес за итни промени.

4.3 Мрежна безбедност

Снабдувачот (Изведувачот) има имплементирано и одржува инфраструктурни компоненти за мрежна безбедност, како што се заштитни ѕидови (firewalls), системи за откривање/спречување напади (IDS/IPS) или други безбедносни контроли кои овозможуваат откривање, континуирано следење и ограничување на мрежниот сообраќај за да се намали влијанието на нападите. Се преземаат построги мерки за системи кои претставуваат поголем ризик (на пр., системи за пристап од надворешни мрежи).

Снабдувачот (Изведувачот) обезбедува спроведување формална политика за далечински пристап.

Далечинскиот пристап на Снабдувачот (Изведувачот) до мрежите и системите на Клиентот е предмет на правилата и условите и безбедносните спецификации доставени за таа цел од страна на Клиентот и зависи од склучувањето посебен договор за далечински пристап.

Снабдувачот (Изведувачот) обезбедува индустриски-стандардизирана сегрегација и сегментација на околините доколку:

(1) околините се споделуваат со други клиенти; и/или
(2) Снабдувачот (Изведувачот) поставува околина за развој, тестирање и користење.

4.4 Енкрипција

Снабдувачот (Изведувачот) обезбедува соодветна заштита на доверливоста на податоците преку примена на криптографски мерки (технологии за шифрирање) на податоците при пренос и во мирување во согласност со водечките стандарди и упатства или еквиваленти и соодветно управување со криптографските клучеви. Сите информации означени како интерни, доверливи и строго доверливи пренесени надвор од компанијата мора да бидат шифрирани.

Снабдувачот (Изведувачот) ги штити мобилните уреди и надворешните електронски медиуми (на пр., USB флеш драјвови, преносливи хард дискови, ленти) од неовластен пристап преку соодветни физички и логички безбедносни мерки. Мора да се обезбеди шифрирање на податоците зачувани на такви уреди.

4.5 Заштита од злонамерен софтвер

Снабдувачот (Изведувачот) користи соодветни и постојано ажурирани алатки за блокирање за да ги заштити серверите и крајните уреди од злонамерен софтвер. Софтверот мора да може да открие дали софтверот за антивирус/злонамерен софтвер на уредите е оневозможен или не е ажуриран редовно.

4.6 Контрола и мониторинг на безбедноста

Снабдувачот (Изведувачот) има имплементирано соодветни безбедносни мерки (особено во однос на сајбер заканите) за податоци, апликации и системи. Снабдувачот (Изведувачот) редовно ја оценува ефективноста на безбедносните мерки во однос на познатите сајбер закани и измами, како и соодветните модели.

Снабдувачот (Изведувачот) планира и спроведува процени на повредите и пенетрациски тестови во редовни интервали за сите системи што се користат за давање услуги на Корисниците. На овие системи мора да се извршат пенетрациски тестови:

(1) најмалку еднаш годишно;
(2) секогаш кога има нова верзија или големо ажурирање на апликации/софтвер/информациски услуги;
(3) само од страна на вешти и искусни тестери со доволно познавање кои не биле вклучени во развојот на безбедносните мерки.

Сите откриени повреди и добиените резултати мора да се управуваат на соодветен начин: анализа, класификација и отстранување. Активностите за отстранување на повредите мора да се спроведат во согласност со критичноста, соодветно брзо во однос на времето на откривање. На барање, Снабдувачот (Изведувачот) обезбедува збирни извештаи за процена на повредата и/или резултатите од пенетрациските тестови.

Снабдувачот (Изведувачот) гарантира дека безбедносните неусогласености пријавени од Клиентот се поправени во разумен временски период.

Клиентот го задржува правото да врши безбедносни процени и прегледи со цел да се потврди усогласеноста со наведените барања. Клиентот се согласува однапред да го извести Снабдувачот (Изведувачот) и гарантира дека ревизијата е спроведена во редовни работни часови со минимално нарушување на работата на Снабдувачот (Изведувачот). На барање, Снабдувачот (Изведувачот) писмено ја потврдува својата усогласеност со наведените барања и писмено одговара на сите прашања што Клиентот може да му ги постави на Снабдувачот (Изведувачот) во врска со неговите безбедносни процедури.

4.7 Зајакнување на системот

Снабдувачот (Изведувачот) ги конфигурира и ги распоредува своите ИТ-ресурси (на пр., бази на податоци, апликации, оперативни системи, мрежни уреди) во согласност со барањата на информативната безбедност и во согласност со најдобрите практики (на пр., CIS стандарди) или еквивалентни стандарди. Конфигурациите на ИТ-средствата редовно се ревидираат и се ажурираат.

5 Оперативност

5.1 Управување со податоци

Снабдувачот (Изведувачот) гарантира дека се преземени мерки против губење и истекување на податоците.

Снабдувачот (Изведувачот) не смее ниту да ги умножува корисничките податоци на клиентите ниту да ги користи во непродукциски околини. Секое користење на податоците на клиентите во непродукциски околини зависи од експлицитната и документирана согласност на клиентот.

Снабдувачот (Изведувачот) гарантира дека, по раскинувањето на договорниот однос, по барање информациите (физички, дигитални) безбедно се бришат или се враќаат медиумите за пренос на информациите.

5.2 Резервни копии и враќање на податоците (Backup & Recovery)

Снабдувачот (Изведувачот) обезбедува постоење на концепти за резервна копија

и зачувување податоци за секоја релевантна платформа/компонента за која е одговорен. Се проверуваат периодите на зачувување и се прават резервни копии, како и тестови за враќање на податоците. Концептот за резервна копија и процедурите за враќање на податоците се од таква природа што ги обезбедуваат договорените нивоа на достапност.

5.3 Евиденција (Logging) и следење (Monitoring)

Снабдувачот (Изведувачот) презема соодветни мерки за да обезбеди транспарентност и следење на сите изведени операции. Евиденцијата (логовите) мора да биде доволно детална за да помогне во идентификација на изворот на (безбедносниот) случај и да овозможи повторно креирање на низата настани. Евиденцијата (логовите) мора да биде достапна на Клиентот ако Клиентот има оправдана причина. Евиденцијата (логовите) мора да ги снима обидите за пристап, информациите во врска со безбедносните настани на системот и мрежата, алармите, дефектите и грешките. Мора да се гарантира интегритет на датотеката за евиденција на логови (log file evidence). Пристапот до датотеката за евиденција на логови мора да биде ограничен.

5.4 Управување со инциденти и известувања

Снабдувачот (Изведувачот) мора да има имплементирано документирани процедури за управување со инциденти за информативната безбедност што овозможуваат ефективно и уредно управување со безбедносните инциденти. Процедурите мора да опфаќаат известување, анализа, следење, решавање и документирање на безбедносните инциденти, како и процеси за реагирање и обновување по безбедносен инцидент.

Снабдувачот (Изведувачот) се согласува да го извести Клиентот веднаш штом ќе дознае за каков било инцидент директно или индиректно поврзан со услугите и податоците на Клиентот преку е-пошта, supplier-incident@evn.mk и да ги достави сите информации што му се познати кои би му помогнале на Клиентот во исполнувањето на неговите обврски. Снабдувачот (Изведувачот) ги обезбедува таквите информации чекор по чекор кога ќе станат достапни. По потврда на безбедносниот инцидент поврзан со услугите или податоците на Клиентот, Снабдувачот (Изведувачот):

i. се согласува дополнително да ги извести деловните единици на Клиентот во писмена форма;
ii. осигурува дека таквото известување ги содржи најмалку следните информации; ако првично не се достапни сите информации, Снабдувачот (Изведувачот) треба да обезбеди детали – во случај на временски критични случаи или непосредна опасност веднаш штом се достапни – во серија известувања:
   - Контакт-информации за лицето одговорно за инцидентот на Снабдувачот (Изведувачот) – Што се случи?
   - Како настана?
   - Зошто се случи?
   - Засегнати компоненти/системи/средства
   - Засегнати услуги/податоци за клиентите
   - Датум и време на настанување на инцидентот
   - Датум и време на откривање на инцидентот
   - Влијание врз бизнисот/влијание врз услугите на клиентите/податоци
   - Решение на инцидент
   - Преземени мерки за разрешување на инцидентот
   - Планирани мерки за разрешување на инцидентот
iii. ги прави сите разумни напори за откривање и спречување такви инциденти;
iv. тековно го известува Клиентот за мерките што ги презема/планира да ги преземе Снабдувачот (Изведувачот);
v. добива претходна писмена согласност од Клиентот според важечкиот закон во врска со секое известување или информации од јавен карактер во врска со таквото прекршување; и
vi. ги координира сите натамошни активности со Клиентот.
vii. Ова барање за известување важи и за подизведувачите.

6 Физичка безбедност

6.1 Физички пристап

Просториите на Снабдувачот (Изведувачот) се категоризирани во различни заштитни зони што одговараат на безбедносните мерки и правата за пристап во согласност со релевантните безбедносни барања.

Физичкиот пристап до ИТ-системите, како што се серверите, дополнително е ограничен со посебни заштитни зони до кои има пристап само овластен персонал.

7 Управување со континуитет на бизнисот (BCM – Business Continuity Management)

7.1 BCM

Снабдувачот (Изведувачот) има имплементирано тековни и континуирано одржувани планови за обнова од катастрофи (disaster recovery) и за воспоставување континуитет во деловното работење. Плановите за обнова од катастрофи и плановите за воспоставување континуитет во деловното работење мора да бидат дизајнирани за да спречат, во најголема можна мера, какви било негативни влијанија од непланирани прекини и да му овозможат на Снабдувачот (Изведувачот), исто така, во случај на прекини, да продолжи да работи и да дава услуги во согласност со неговиот договор со Клиентите. На барање, Снабдувачот (Изведувачот) му дава на Клиентот писмени резимеа за неговите планови за обнова од катастрофи и за воспоставување континуитет во деловното работење.

Најмалку еднаш годишно, Снабдувачот (Изведувачот) спроведува соодветни тестови на континуитетот на сопственото деловно работење и плановите за обнова од катастрофи. Резултатите од тестовите кои се релевантни за услугата му се достапни на Клиентот на барање и откако ќе бидат извршени таквите тестови.

Снабдувачот (Изведувачот) се грижи опсегот на плановите за воспоставување континуитет на деловното работење и за обнова од катастрофи да ги опфаќа сите локации, вработени и информациски системи што се користат за давање услуги на Клиентот.

8 Исполнување на безбедносните барања

Прифаќањето на безбедносните барања од двете страни е предуслов за склучување договор.

Во случај добавувачот да не исполни некои од условите, Купувачот има право да ги прифати, давајќи писмено оправдување за прифаќањето.