Резиме на Општите безбедносни политики на Групацијата за осигурување Сава

Љубљана, април 2025 год.

Содржина

1 ВОВЕД 3
2 ЦЕЛ И ОПФАТ НА БЕЗБЕДНОСНИТЕ ПОЛИТИКИ 3
3 ОПШТИ БАРАЊА 3
4 УПРАВУВАЊЕ СО ПРИСТАПОТ 3
5 ЗАШТИТА НА ПОДАТОЦИ 4
6 УПРАВУВАЊЕ СО ИНЦИДЕНТИ 4
7 ОТПОРНОСТ И КОНТИНУИТЕТ 5
8 УПРАВУВАЊЕ СО ПОИЗВЕДУВАЧИ, ПОВРЗАНИ СО ДОГОВОРНАТА УСЛУГА 5
9 РЕВИЗИЈА И ПРОЦЕНА НА РИЗИЦИТЕ 5
10 ЕДУКАЦИЈА И КРЕВАЊЕ НА СВЕСТА 5
11 ПРЕСТАНУВАЊЕ НА СОРАБОТКАТА 5
12 АЖУРИРАЊА И ИЗМЕНИ 5
13 ПОИМИ И СКРАТЕНИЦИ 6

1 ВОВЕД

Во овој документ се резимирани клучните безбедносни политики на Групацијата за осигурување Сава (во продолжение ГОС), приспособени за јавно објавување за потребите на добавувачите. Тој е наменет за сите договорни партнери, коишто при својата работа и за извршување на договорните услуги пристапуваат кон какви било ИКТ ресурси на ГОС (на пр. апликации, средства за телекомуникации, збирки на податоци и др.) или ги користат.

Ова резиме ги опфаќа следните содржини:

- правилно користење на сите информациски ресурси, односно ИКТ ресурси,
- управување со информациските ресурси, односно ИКТ ресурсите,
- електронско работење,
- обезбедување на опремата и информациските ресурси,односно ИКТ ресурсите.

Со усвојувањето на Општите безбедносни политики на ГОС добавувачот (договорниот партнер) се обврзува дека при спроведувањето на договорните обврски ќе ги почитува безбедносните барања на информатичката технологија во согласност со важечките добри практики, минималните стандарди и начелата на струката, како и важечките прописи.

2 ЦЕЛ И ОПФАТ НА БЕЗБЕДНОСНИТЕ ПОЛИТИКИ

Целта на безбедносните политики во ГОС е следната:

- обезбедување на безбедно и соодветно користење на ИКТ ресурсите,
- запознавање на корисниците со ризиците, поврзани со користењето на ИКТ ресурсите,
- определување на мерки за заштита на информациите од неовластено обелоденување или злоупотреба.

Договорните корисниците мора сите ИКТ ресурси на ГОС да ги користат совесно, ефикасно и одговорно.

ГОС во најголема можна мера ги заштитува вработените и својата сопственост од незаконити или штетни намерни или ненамерни активности на лица.

Несоодветното користење на информатичката технологија ја изложува ГОС и нејзините корисници на ризици, како што се заразување на информатичката технологија со компјутерски вируси, загрозување на мрежните системи и услуги и злоупотреба на информациите и податоците, зачувани во информацискиот систем на ГОС.

3 ОПШТИ БАРАЊА

- Добавувачот мора да ги почитува сите важечки закони и прописи, вклучувајќи ја и Општата уредба за заштита на податоците (ГДПР) и Уредбата за дигитална оперативна отпорност за финансискиот сектор (ДОРА).
- Добавувачот мора да назначи лице за контакт за безбедносни комуникации и одговор на инциденти.

4 УПРАВУВАЊЕ СО ПРИСТАПОТ

- Добавувачот мора да воспостави строги контроли за спречување на пристапот до ИКТ системите на ГОС на неовластени лица.

- Добавувачот мора да воспостави строги контроли, со што ќе обезбеди до ИКТ системите на ГОС да пристапуваат само овластени лице, коишто се соодветно проверени и обучени.
- Управувањето со пристапите се однесува на сите форми на пристап до ИКТ ресурсите, коишто меѓу другото вклучуваат:
    - кориснички пристапи преко кориснички интерфејси (ГУИ),
    - пристапи преку програмски интерфејси (АПИ),
    - системски/услужни пристапи (сервисни сметки),
    - администраторски и привилегирани пристапи,
    - скрипти, временски работи (англ. cron job) и автоматизирани интеграции,
    - пристапи на далечина (ВПН, РДП, ССХ и др.),
    - пристапи преку мобилни уреди или облак.
- Заштитата на пристапите до ИКТ системите на ГОС, меѓу другото, вклучува повеќефакторска автентикација (МФА) и примена на начелото на најмала привилегија (англ. least privilege).
- Сите пристапи до системите или податоците, поврзани со ГОС, заради обезбедување на ревизиска трага се бележат и се следат.
- Добавувачот мора да одржува ажуриран список на овластениот персонал со права на пристап до ИКТ системите на ГОС и редовно да го проверува.

5 ЗАШТИТА НА ПОДАТОЦИ

- Добавувачот мора да обезбеди интегритет, доверливост и расположливост на податоците.
- Сите податоци во текот на преносот мора да бидат шифрирани со примена на криптографскиот протокол ТЛС 1.2 или понова верзија.
- Сите податоци во мирување, влчучувајќи ги и сигурносните копии, мора да бидат шифрирани со примена на стандардот АЕС -256 или еквивалентен стандард.
- Добавувачот мора да обезбеди работните компјутери, коишто се користат за вршење на договорната услуга, да бидат редовно безбедносно ажурирани, да имаат инсталирано исклучиво законита програмска опрема и да бидат заштитени со редовно ажуриран антивирусен систем.
- Добавувачот мора да обезбеди минимизација на обработката и зачувувањето на податоците, при што смее да обработува и да зачувува само податоци, коишто се неопходни за извршување на договорните обврски.
- Добавувачот мора да избегнува непотребно зачувување на податоците и да обезбеди податоците да се бришат или анонимизираат веднаш по престанувањето на потребата од зачувување.
- Добавувачот при престанување на договорниот однос мора податоците безбедно да ги избрише или во целост да ѝ ги врати на ГОС.

6 УПРАВУВАЊЕ СО ИНЦИДЕНТИ

- Добавувачот мора да има политика за управување со инциденти, којашто вклучува откривање, известување и решавање на безбедносни инциденти.
- Безбедносните инциденти на добавувачот, коишто влијаат на ГОС мора да бидат пријавени во ГОС во рок од 24 часа.
- Добавувачот мора на ГОС да ѝ овозможи учество во решавањето на инцидентот, којшто има влијание на ИКТ системот, вклучувајќи обезбедување на пристап до соодветна документација.

7 ОТПОРНОСТ И КОНТИНУИТЕТ

- Добавуачот мора да има воспоставен план за континуитет во работењето (англ. Business Continuity Plan – BCP) и план за одговор на катастрофи (англ. Disaster Recovery Plan – DRP), коишто вклучуваат периодично тестирање,
- Плановите треба да се тестираат еднаш годишно, а резултатите да се споделуваат со ГОС на нејзино барање.

8 УПРАВУВАЊЕ СО ПОИЗВЕДУВАЧИ, ПОВРЗАНИ СО ДОГОВОРНАТА УСЛУГА

- Добавувачот мора да добие писмена согласност од нарачателот (ГОС) пред вклучување на подизведувачи или трети лица.
- Добавувачот мора да обезбеди сите подизведувачи да исполнуваат исти барања, како што би требало да ги исполнува самиот тој.

9 РЕВИЗИЈА И ПРОЦЕНА НА РИЗИЦИТЕ

- Добавувачот мора да врши редовни процени на ризиците, поврзани со своите услуги, и да го вклучи нарачателот (ГОС) во оценувањето, каде што тоа е соодветно.
- Нарачателот (ГОС) за добавувачот мора да подготви процена на ризикот, што може да вклучива доставување на безбедносни прашалници до добавувачот и вршење на независни проверки на безбедносните мерки.
- Добавувачот мора на барање на нарачателот да достави извештаи за своите ревизии и тестирања, да достави одговори на безбедносните прашалници и разумно да учествува во вршењето на независните проверки.
- Нарачателот (ГОС) има право да врши редовни ревизии и независни проверки на безбедносните мерки на добавувачот.
- Добавувачот мора на барање на ГОС да достави докази за сообразност, како што се сертификати, извештаи или резултати во врска со безбедносните тестови.

10 ЕДУКАЦИЈА И КРЕВАЊЕ НА СВЕСТА

- Добавувачот мора редовно да ги обучува своите вработени, коишто работат за нарачателот (ГОС), во врска со добрите практики од областа на информацискатa безбедност и други содржини, ако тоа го бара нарачателот (ГОС).

11 ПРЕСТАНУВАЊЕ НА СОРАБОТКАТА

- По престанувањето на договорот, добавувачот мора да обезбеди безбедно исклучување на услугите од ИКТ системот на ГОС, вклучувајќи укинување на пристапите и безбедно бришење на сите податоци на ГОС.
- По престанувањето на договорот добавувачот мора да достави изјава или друг доказ за бришење на податоците.

12 АЖУРИРАЊА И ИЗМЕНИ

- ГОС го задржува правото да го ажурира овој документ, со што ќе се обезбеди одговор на промените на ризиците, технологијата или прописите. Добавувачот ќе биде известен за ажурирањата и во разумно време ќе мора да обезбеди усогласеност.

13 ПОИМИ И СКРАТЕНИЦИ

Бр.	Поим/скратениве	Опис
3	**ГОС**	Групација за осигурување Сава
4	**ИКТ**	Информатичко-комуникациска технологија – технологија, којашто овозможува прибирање, обработка и размена на податоци
5	**МФА**	Multi-Factor Authentication – повеќестепена автентикација за зголемување на безбедноста на пристапот
7	**AEC256**	Advanced Encryption Standard (256-bit) – криптографски алгоритам за шифрирање за заштита на податоците во мирување
8	**ТЛС 1.2**	Transport Layer Security 1.2 – криптографски протокол за безбедна комуникација во мрежите