Policy för samordnad rapportering av sårbarheter

SGA Conveyor System AB

Version	**1.2**
Gäller från och med	**11 september 2026**
Klassificering	**Offentlig – för publicering på sga-conveyor.se**

INNEHÅLLSFÖRTECKNING

1. Syfte

Säkerheten i våra produkter och tjänster samt våra kunders säkerhet har högsta prioritet för SGA Conveyor System AB.

Trots omsorgsfull utveckling, kvalitetssäkring samt tekniska och organisatoriska säkerhetsåtgärder kan förekomsten av sårbarheter inte helt uteslutas.

Denna samordnade policy för rapportering av sårbarheter (nedan kallad ”CVD-policyn” eller ”policyn”) beskriver hur externa säkerhetsforskare, kunder och andra parter kan rapportera möjliga säkerhetssårbarheter i SGA Conveyor System AB:s produkter, applikationer och tjänster samt hur SGA Conveyor System AB hanterar sådana rapporter.

Syftet med policyn är att säkerställa en ansvarsfull, samordnad och transparent hantering av rapporterade sårbarheter för att minimera riskerna för kunder, system och allmänheten.

2. Tillämpningsområde

2.1 OMFATTNING

Policyn gäller alla produkter med digitala element som tillverkas av SGA Conveyor System AB, släpps ut på marknaden inom EU eller används inom EU.

2.2 UNDANTAG

- System, installationer eller andra enheter som inte ägs av de parter som omfattas av denna policy.

Om sårbarheter upptäcks eller misstänks i system som inte omfattas av denna policy ska de rapporteras direkt till respektive tillverkare, operatör eller behörig myndighet.

3. Rapportering av en säkerhetssårbarhet

Säkerhetssårbarheter kan rapporteras på följande sätt:

> **E-POST**
>
> product-security@bowe.com

För att möjliggöra snabb handläggning ska rapporten innehålla följande information:

- Berörd produkt eller berört system
- Berörd kund (namn, ordernummer), om tillämpligt
- Produktversion
- Beskrivning av sårbarheten
- Uppgift om huruvida det finns kännedom om att sårbarheten aktivt utnyttjas
- Steg för att återskapa sårbarheten
- Koncepttest (proof of concept), om tillgängligt
- Kontaktuppgifter för frågor

Lämna endast den information som är nödvändig för att bedöma sårbarheten och avstå från att skicka onödiga personuppgifter eller konfidentiella uppgifter om tredje part.

Rapporten kan lämnas på tyska eller engelska.

4. Våra åtaganden

Om du samarbetar med oss i enlighet med denna policy kan du förvänta dig att vi:

- bekräftar mottagandet av din rapport inom fem arbetsdagar och samarbetar med dig för att undersöka och validera den rapporterade sårbarheten.
- i den utsträckning det är möjligt och lämpligt håller dig informerad om hur vår utredning fortskrider.
- skyndsamt åtgärdar identifierade sårbarheter med beaktande av operativa och tekniska begränsningar, eller genomför lämpliga riskreducerande åtgärder.
- ger det skydd för säkerhetsforskare som beskrivs i kapitel 5 och 6 för säkerhetsforskning som bedrivs i enlighet med dessa kapitel.

5. Förväntat agerande av säkerhetsforskare

Vi välkomnar säkerhetsforskning som utförs i god tro och ber att följande regler följs. Fullständig efterlevnad av dessa regler är en förutsättning för det skydd för säkerhetsforskare som beskrivs i kapitel 6.

5.1 TILLÅTNA AKTIVITETER

- Identifiering och dokumentation av säkerhetssårbarheter
- Genomförande av minsta möjliga testning som krävs för verifiering
- Rapportering av sårbarheten uteslutande till SGA Conveyor System AB via den rapporteringskanal som anges i kapitel 3
- Konfidentiell behandling av iakttagelser
- Säkerhetsundersökningar i egna testmiljöer eller i miljöer där uttryckligt tillstånd har lämnats

5.2 FÖRBJUDNA AKTIVITETER

- Åtkomst till tredje parts uppgifter
- Ändring eller radering av uppgifter
- Avbrott i tjänster
- Överbelastningsattacker (denial-of-service)
- Social manipulation riktad mot anställda eller kunder
- Installation av skadlig kod
- Fysisk manipulering av kundutrustning
- Testning i kunders produktionssystem utan deras uttryckliga samtycke
- Tester på maskiner i drift
- Manipulering av PLC-, CNC-, robot- eller maskinstyrsystem
- Ändringar av processparametrar
- Kringgående av säkerhets- eller skyddsfunktioner
- Aktiviteter som kan påverka arbetsmiljö, anläggningssäkerhet eller produktkvalitet
- Belastnings- eller stresstester på OT-system i produktion

5.3 FÖRFARANDE VID OAVSIKTLIG ÅTKOMST TILL UPPGIFTER

Om känsliga uppgifter eller personuppgifter oavsiktligt blir åtkomliga under testaktiviteter ska alla aktiviteter omedelbart avbrytas. Händelsen ska dokumenteras som en del av rapporteringen. De berörda uppgifterna får inte granskas, lagras, behandlas vidare eller lämnas ut.

6. Skydd för säkerhetsforskare (safe harbor)

Vi avser inte att vidta rättsliga åtgärder mot säkerhetsforskare som agerar i god tro och i enlighet med denna policy.

6.1 FÖRUTSÄTTNINGAR

Det skydd för säkerhetsforskare som beskrivs i detta kapitel gäller endast om och i den utsträckning den rapporterande personen fullständigt och fortlöpande följer samtliga villkor i kapitel 5, särskilt att personen:

- uteslutande ägnar sig åt de aktiviteter som anges som tillåtna i avsnitt 5.1,
- inte ägnar sig åt någon av de aktiviteter som anges som förbjudna i avsnitt 5.2,
- agerar omedelbart vid oavsiktlig åtkomst till känsliga uppgifter eller personuppgifter enligt avsnitt 5.3, och
- rapporterar sårbarheten uteslutande via den rapporteringskanal som anges i kapitel 3.

6.2 ÅTAGANDETS OMFATTNING

Under förutsättning att kraven i avsnitt 6.1 är uppfyllda betraktar vi den säkerhetsforskning som genomförts inom ramen för rapporten som en aktivitet godkänd av SGA Conveyor System AB.

Vi kommer inte att vidta några civilrättsliga eller straffrättsliga åtgärder mot den rapporterande personen med anledning av upptäckten, undersökningen och rapporteringen av sårbarheten. Vi kommer dessutom att göra vad som står i vår makt för att tredje part också ska avstå från sådana åtgärder, förutsatt att de relevanta aktiviteterna utfördes för den rapporterande personens räkning och på dennes begäran i enlighet med denna policy.

6.3 BEGRÄNSNINGAR AV ÅTAGANDET

Detta åtagande:

- gäller endast den specifika sårbarhet som rapporterats och de aktiviteter som är nödvändiga för att verifiera den;
- skapar inte något separat anspråk gentemot tredje part (t.ex. berörda kunder) och påverkar inte deras egna rättigheter;
- gäller inte handlingar som strider mot tillämplig lag oberoende av denna policy;
- kan när som helst ändras av SGA Conveyor System AB för framtida rapporter; rapporter som redan har lämnats i enlighet med reglerna påverkas inte av senare ändringar.

7. Bedömning och prioritering

Vi strävar efter att bedöma och besvara inkommande rapporter skyndsamt.

Varje rapporterad sårbarhet bedöms särskilt utifrån följande kriterier:

- Möjlighet att utnyttja sårbarheten

- Påverkan på konfidentialitet
- Påverkan på informationens riktighet och integritet
- Påverkan på tillgänglighet
- Påverkan på funktionssäkerhet

8. Samordnat offentliggörande

Vi föredrar ett samordnat offentliggörande av sårbarheter. Standardförfarandet är följande:

1. Mottagande av rapporten
2. Analys och riskbedömning
3. Utveckling av en korrigering eller riskreducerande åtgärd
4. Tillhandahållande av en uppdatering
5. Information till berörda kunder
6. Publicering av ett säkerhetsmeddelande

Vi ber rapportörer att avstå från att offentliggöra problemet tills en korrigering har tillhandahållits eller ett annat tillvägagångssätt har överenskommits gemensamt.

I de fall som krävs enligt lag (särskilt vid aktivt utnyttjade sårbarheter eller allvarliga säkerhetsincidenter) kan SGA Conveyor System AB omfattas av ytterligare lagstadgade underrättelse- och rapporteringsskyldigheter gentemot behöriga myndigheter. Denna policy påverkar inte sådana skyldigheter.

9. Hantering av rapporter

Vi värdesätter ansvarsfull rapportering högt. SGA Conveyor System AB bedriver för närvarande inget bug bounty-program och lämnar ingen ekonomisk ersättning för sårbarhetsrapporter.

10. Dataskydd

Personuppgifter som lämnas i samband med en sårbarhetsrapport används uteslutande för att behandla rapporten.

Behandlingen sker i enlighet med tillämpliga dataskyddsbestämmelser, särskilt den allmänna dataskyddsförordningen (GDPR).

Uppgifterna görs endast tillgängliga för dem som deltar i utredningen och raderas eller arkiveras efter att processen har slutförts i enlighet med våra interna gallrings- och lagringsrutiner.

Mer information om behandling av personuppgifter finns i vår integritetspolicy på sga-conveyor.se.