POLITIKA KOORDINOVANÉHO ZVEŘEJŇOVÁNÍ ZRANITELNOSTÍ

COORDINATED VULNERABILITY DISCLOSURE POLICY

Verze / Version	1.0
Účinnost / Effective date	Dnem zveřejnění / Date of publication
Vlastník / Document owner	HQ Systems s.r.o.
Bezpečnostní kontakt / Security contact	security@hqsystems.cz

Veřejná politika pro bezpečné hlášení, posuzování a koordinované zveřejňování zranitelností výrobků, jednoúčelových strojů a softwaru HQ Systems.

Obsah / Table of contents

ČESKÁ VERZE

1. Účel politiky
2. Rozsah politiky
3. Kontakt pro hlášení
4. Obsah hlášení
5. Pravidla bezpečného testování
6. Zpracování hlášení a komunikační lhůty
7. Náprava a koordinované zveřejnění
8. Předání informací a ochrana identity
9. Poděkování, odměny a právní postavení
10. Regulatorní oznamování
11. Změny politiky a rozhodné znění

ENGLISH VERSION

1. Purpose of this policy
2. Scope
3. Reporting contact
4. Information to include
5. Rules for safe testing
6. Report handling and communication timeframes
7. Remediation and coordinated disclosure
8. Information sharing and protection of identity
9. Acknowledgement, rewards, and legal status
10. Regulatory reporting
11. Policy updates and prevailing language

ČESKÁ VERZE

1. ÚČEL POLITIKY

Společnost HQ Systems s.r.o. bere bezpečnost svých výrobků, jednoúčelových strojů a vlastního softwaru vážně. Tato politika stanoví pravidla pro koordinované oznamování, posuzování, řešení a případné zveřejňování bezpečnostních zranitelností.

Cílem politiky je umožnit zákazníkům, uživatelům a bezpečnostním výzkumníkům oznámit možnou zranitelnost způsobem, který umožní její bezpečné ověření a nápravu a současně nebude ohrožovat osoby, provoz strojů, dostupnost systémů, důvěrnost informací ani práva třetích stran.

Tato politika není určena pro běžné servisní požadavky, technickou podporu, reklamace, obchodní nabídky, obecné dotazy ani hlášení čistě mechanických nebo provozních závad bez souvislosti s kybernetickou bezpečností.

2. ROZSAH POLITIKY

Tato politika se vztahuje na bezpečnostní zranitelnosti:

a) výrobků a zařízení uvedených na trh společností HQ Systems s.r.o.;

b) jednoúčelových strojů uvedených na trh společností HQ Systems s.r.o.;

c) jednoúčelových strojů dodaných společností HQ Systems s.r.o. zákazníkovi v režimu OEM, pokud v době přijetí hlášení existuje smluvní vztah, na jehož základě HQ Systems s.r.o. odpovídá za dotčenou část stroje, software, podporu nebo řešení bezpečnostní zranitelnosti;

d) softwaru vyvinutého společností HQ Systems s.r.o., včetně firmwaru, desktopových aplikací, obslužného softwaru a dalších softwarových součástí dodaných jako součást výrobku nebo stroje.

U OEM dodávek se rozsah této politiky omezuje na části, které vyvinula, dodala nebo za které podle příslušného smluvního vztahu odpovídá společnost HQ Systems s.r.o. Odpovědnost za ostatní části může nést OEM zákazník, provozovatel stroje nebo příslušný dodavatel.

Do rozsahu nespadají zejména:

e) výrobky, komponenty, služby nebo software třetích stran, které nebyly vyvinuty ani dodány společností HQ Systems s.r.o., s výjimkou případu, kdy jsou integrovány do výrobku firmou HQ Systems a zranitelnost může ovlivnit bezpečnost tohoto výrobku;

f) veřejné webové stránky, e-mailové služby a interní informační systémy HQ Systems s.r.o., pokud nejsou výslovně součástí dodaného výrobku, stroje nebo vlastního softwaru;

g) systémy a zařízení, k jejichž testování nemá oznamovatel vlastnické právo nebo prokazatelné písemné oprávnění;

h) požadavky na poskytnutí nové funkce nebo běžné servisní podpory pro produkty po skončení podpory. Bezpečnostní zjištění týkající se takového produktu lze oznámit a HQ Systems s.r.o. je posoudí podle rizika, avšak přijetí hlášení samo o sobě nezakládá nárok na aktualizaci nebo opravu, pokud taková povinnost nevyplývá z právního předpisu nebo smlouvy.

Pokud si oznamovatel není jistý, zda zjištění spadá do rozsahu této politiky, může před zahájením dalšího testování zaslat stručný dotaz na bezpečnostní kontakt.

3. KONTAKT PRO HLÁŠENÍ

Bezpečnostní zranitelnosti oznamujte výhradně na:

security@hqsystems.cz

Tato e-mailová adresa slouží výhradně pro hlášení bezpečnostních zranitelností výrobků, zařízení, jednoúčelových strojů a softwaru v rozsahu této politiky. Není určena pro technickou podporu, servisní požadavky, reklamace, obchodní nabídky ani obecné dotazy.

Doporučený předmět zprávy:

Hlášení zranitelnosti – [typové číslo zařízení]

Komunikace probíhá prostřednictvím e-mailu. Oznamovatel nemá zasílat hesla, soukromé klíče, přístupové údaje, osobní údaje, kompletní provozní databáze ani jiné citlivé informace, pokud nejsou pro prvotní posouzení nezbytné. Je-li nutné předat citlivější technické podklady, doporučujeme nejprve zaslat jejich popis a vyčkat na další pokyny.

4. OBSAH HLÁŠENÍ

Hlášení by mělo obsahovat alespoň následující informace:

i) typové číslo ze štítku zařízení; tento údaj je povinný, pokud se hlášení týká konkrétního zařízení nebo stroje;

j) sériové nebo výrobní číslo zařízení, je-li k dispozici;

k) název výrobku, stroje, softwaru nebo dotčené součásti;

l) verzi firmwaru, softwaru, operačního systému nebo konfigurace;

m) stručný a věcný popis zranitelnosti;

n) možný dopad na důvěrnost, integritu, dostupnost, funkci stroje nebo bezpečnost osob;

o) postup umožňující problém reprodukovat nebo ověřit;

p) ověřovací kód, důkaz konceptu, snímky obrazovky, fotografie štítku, relevantní výpisy protokolů nebo jiné podpůrné podklady, jsou-li dostupné;

q) informaci, zda je zranitelnost veřejně známá, zda byla sdělena jiné osobě nebo zda existují známky jejího aktivního zneužívání;

r) datum a přibližný čas zjištění;

s) kontaktní údaje oznamovatele pro následnou komunikaci.

Hlášení má obsahovat pouze informace nezbytné pro identifikaci, posouzení a řešení zranitelnosti. Osobní údaje a provozní data třetích stran mají být odstraněny nebo anonymizovány, kdykoli je to možné.

5. PRAVIDLA BEZPEČNÉHO TESTOVÁNÍ

Oznamovatel smí provádět testování pouze:

- **t)** na zařízení, které vlastní; nebo
- **u)** na zařízení, systému či licenci, k jejichž testování má předchozí prokazatelné písemné oprávnění vlastníka a případně také provozovatele.

Oznamovatel musí při testování postupovat přiměřeně, obezřetně a v rozsahu nezbytném k potvrzení existence zranitelnosti.

Zakázány jsou zejména následující činnosti:

- **v)** testování na strojích nebo systémech v aktivním výrobním provozu bez předchozího písemného souhlasu vlastníka a provozovatele;
- **w)** vyřazení, změna, obcházení nebo zkoušení mezních stavů bezpečnostních funkcí, ochranných zařízení, nouzového zastavení nebo řídicích funkcí způsobem, který by mohl ohrozit osoby nebo majetek;
- **x)** způsobení odstávky, omezení dostupnosti, zahlcení služby, poškození zařízení nebo ztráty či změny dat;
- **y)** získávání, stahování, kopírování, změna nebo zveřejnění dat nad rámec minimálně nezbytný k potvrzení zranitelnosti;
- **z)** přístup k účtům, datům nebo systémům třetích stran;
- **aa)** sociální inženýrství, phishing, fyzické narušení objektů, podvodné jednání nebo kontaktování zaměstnanců mimo bezpečnostní kontakt;
- **bb)** použití zranitelnosti k získání výhody, finančního prospěchu, vydírání nebo požadování odměny;
- **cc)** instalace škodlivého kódu, zachování skrytého přístupu nebo další šíření zranitelnosti;
- **dd)** zveřejnění technických podrobností před koordinovaným vyřešením případu.

Pokud testování může ovlivnit funkční bezpečnost stroje, musí být zastaveno a zjištění musí být bezodkladně oznámeno. Další ověřování je možné pouze v bezpečném, odděleném prostředí a s odpovídajícím oprávněním.[1]

6. ZPRACOVÁNÍ HLÁŠENÍ A KOMUNIKAČNÍ LHŮTY

HQ Systems s.r.o. se bude snažit:

- **ee)** potvrdit přijetí hlášení do 7 kalendářních dnů;

[1] Nařízení (EU) 2024/2847, Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02024R2847-20241120

ff) provést prvotní posouzení a sdělit oznamovateli základní stanovisko do 30 kalendářních dnů od přijetí dostatečně úplného hlášení;

gg) u otevřeného případu poskytnout další informaci o stavu nejméně jednou za 60 kalendářních dnů, pokud to dovoluje povaha případu, smluvní a zákonné povinnosti a ochrana citlivých informací.

Tyto lhůty jsou cílové komunikační lhůty, nikoli záruka úplného odstranění zranitelnosti v uvedené době. Začátek nebo běh lhůty může být ovlivněn neúplným hlášením, nutností získat další informace, nedostupností zařízení, potřebou koordinace s OEM zákazníkem nebo dodavatelem, složitostí zkoušek, požadavky funkční bezpečnosti nebo právními omezeními.

HQ Systems s.r.o. určí prioritu podle závažnosti a pravděpodobnosti zneužití, dopadu na bezpečnost osob a provozu, rozsahu dotčených výrobků, dostupnosti zmírňujících opatření a známek aktivního zneužívání.

Hlášení týkající se aktivně zneužívané zranitelnosti, závažného bezpečnostního incidentu nebo bezprostředního ohrožení osob či provozu může být zpracováno ve zrychleném režimu. Dobrovolné komunikační lhůty podle této politiky neprodlužují ani nenahrazují kratší lhůty stanovené právními předpisy pro oznámení příslušným orgánům.

7. NÁPRAVA A KOORDINOVANÉ ZVEŘEJNĚNÍ

Způsob a časový plán nápravy se stanoví individuálně s ohledem na riziko, technickou složitost, funkční bezpečnost, dostupnost náhradních opatření, validaci změny, distribuci aktualizace, smluvní odpovědnosti a případnou koordinaci s OEM zákazníkem nebo dodavatelem komponenty.

Tato politika nestanoví automatickou pevnou lhůtu pro veřejné zveřejnění. Datum a rozsah zveřejnění se určují případ od případu, zejména podle:

hh) závažnosti a dopadu zranitelnosti;

ii) existence aktivního zneužívání;

jj) dostupnosti opravy nebo účinného zmírňujícího opatření;

kk) času potřebného pro ověření, validaci a bezpečné nasazení nápravy;

ll) rizika, že předčasné zveřejnění zvýší ohrožení uživatelů nebo bezpečnost osob;

mm) zákonných oznamovacích a informačních povinností;

nn) oprávněných zájmů dotčeného OEM zákazníka, provozovatele nebo dodavatele.

Oznamovatel je žádán, aby zranitelnost ani její technické podrobnosti nezveřejňoval bez předchozí písemné koordinace s HQ Systems s.r.o.

HQ Systems s.r.o. může zveřejnění odložit, pokud by bezpečnostní rizika zveřejnění převážila nad jeho přínosy, zejména dokud dotčení uživatelé nedostanou přiměřenou možnost použít dostupnou opravu nebo zmírňující opatření.

Pokud je vydána bezpečnostní aktualizace nebo jiné nápravné opatření, HQ Systems s.r.o. poskytne dotčeným uživatelům informace v rozsahu a čase odpovídajícím příslušným právním,

bezpečnostním a smluvním požadavkům.

8. PŘEDÁNÍ INFORMACÍ A OCHRANA IDENTITY

HQ Systems s.r.o. může v nezbytném rozsahu předat technické informace z hlášení:

- **oo)** dotčenému OEM zákazníkovi nebo provozovateli;
- **pp)** výrobci nebo dodavateli dotčené komponenty;
- **qq)** odborným poradcům zapojeným do ověření nebo nápravy;
- **rr)** příslušnému CSIRT, agentuře ENISA nebo jinému příslušnému orgánu;
- **ss)** jiné osobě, pokud je to nezbytné pro řešení zranitelnosti, ochranu osob, splnění smluvní povinnosti nebo dodržení právních předpisů.

Identita a přímé kontaktní údaje oznamovatele nebudou třetím stranám sděleny bez jeho předchozího souhlasu, pokud takové sdělení nevyžaduje právní předpis, rozhodnutí příslušného orgánu nebo nezbytná ochrana před závažným a bezprostředním ohrožením.

Je-li možné případ vyřešit bez předání identity oznamovatele, budou třetím stranám předány pouze nezbytné technické informace. Tím není dotčeno zákonné zpracování, uchování nebo předání údajů.

9. PODĚKOVÁNÍ, ODMĚNY A PRÁVNÍ POSTAVENÍ

HQ Systems s.r.o. může oznamovateli za řádné a užitečné hlášení poděkovat. Tato politika nezakládá nárok na finanční ani jinou odměnu, veřejné uvedení jména, zaměstnání nebo jinou protihodnotu.

HQ Systems s.r.o. v současnosti neprovozuje program odměn za nalezené chyby (bug bounty).

Tato politika nepředstavuje obecné oprávnění k přístupu do zařízení, systémů nebo dat HQ Systems s.r.o., jejích zákazníků ani třetích stran. Nepředstavuje ani příslib, že HQ Systems s.r.o. neuplatní svá práva v případě jednání, které překročí pravidla této politiky, způsobí škodu, ohrozí osoby nebo provoz, poruší smlouvu či právní předpis nebo zasáhne do práv třetích stran.

10. REGULATORNÍ OZNAMOVÁNÍ

HQ Systems s.r.o. může mít povinnost oznámit aktivně zneužívanou zranitelnost, závažný incident nebo jiné skutečnosti příslušnému CSIRT, agentuře ENISA, orgánu dozoru, zákazníkovi nebo jiné osobě ve lhůtách stanovených právními předpisy nebo smlouvou.[2]

Lhůty 7, 30 a 60 dnů uvedené v této politice se týkají komunikace s oznamovatelem. Neomezují, neprodlužují ani nenahrazují zákonné oznamovací lhůty, povinnost řešit zranitelnosti bez zbytečného odkladu ani povinnost přijmout opatření nezbytná k ochraně osob, výrobků, systémů a dat.

[2]Regulation (EU) 2024/2847, Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02024R2847-20241120

11. ZMĚNY POLITIKY A ROZHODNÉ ZNĚNÍ

HQ Systems s.r.o. může tuto politiku aktualizovat, zejména v návaznosti na změny právních předpisů, výrobků, smluvních vztahů, technických možností nebo interních procesů. Aktuální verze bude zveřejněna na webových stránkách HQ Systems s.r.o.

V případě rozdílu mezi českým a anglickým zněním je rozhodující české znění.

ENGLISH VERSION

1. PURPOSE OF THIS POLICY

HQ Systems s.r.o. takes the security of its products, special-purpose machinery, and proprietary software seriously. This policy defines the rules for the coordinated reporting, assessment, remediation, and possible disclosure of security vulnerabilities.

The purpose of this policy is to allow customers, users, and security researchers to report a potential vulnerability in a manner that enables safe verification and remediation without endangering people, machinery operations, system availability, confidentiality of information, or third-party rights.

This policy is not intended for ordinary service requests, technical support, warranty claims, sales offers, general enquiries, or reports of purely mechanical or operational defects with no cybersecurity relevance.

2. SCOPE

This policy applies to security vulnerabilities in:

a) products and equipment placed on the market by HQ Systems s.r.o.;

b) special-purpose machinery placed on the market by HQ Systems s.r.o.;

c) special-purpose machinery supplied by HQ Systems s.r.o. to an OEM customer, provided that, at the time the report is received, a contractual relationship exists under which HQ Systems s.r.o. is responsible for the affected part of the machinery, software, support, or remediation of the security vulnerability;

d) software developed by HQ Systems s.r.o., including firmware, desktop applications, operator software, and other software components supplied as part of a product or machine.

For OEM deliveries, the scope of this policy is limited to the parts developed or supplied by HQ Systems s.r.o., or for which HQ Systems s.r.o. is responsible under the applicable contractual relationship. Responsibility for other parts may rest with the OEM customer, machinery operator, or relevant supplier.

The following are generally out of scope:

e) third-party products, components, services, or software not developed or supplied by HQ Systems s.r.o., unless they are integrated into an HQ Systems product and the vulnerability may affect the security of that product;

f) public websites, email services, and internal information systems of HQ Systems s.r.o., unless they are expressly part of a supplied product, machine, or proprietary software;

g) systems and devices that the reporter does not own and is not demonstrably authorised in writing to test;

h) requests for new functionality or ordinary service support for products that are no longer supported. Security findings concerning such a product may still be reported and will be assessed by HQ Systems s.r.o. according to risk, but acceptance of the report does not by itself create an entitlement to an update or fix unless required by law or contract.

If a reporter is unsure whether a finding falls within the scope of this policy, they may send a brief enquiry to the security contact before performing any further testing.

3. REPORTING CONTACT

Report security vulnerabilities exclusively to:

security@hqsystems.cz

This email address is exclusively for reporting security vulnerabilities in products, equipment, special-purpose machinery, and software within the scope of this policy. It is not intended for technical support, service requests, warranty claims, sales offers, or general enquiries.

Recommended email subject:

Vulnerability report – [device type number]

Communication takes place by email. Reporters must not send passwords, private keys, credentials, personal data, complete operational databases, or other sensitive information unless strictly necessary for the initial assessment. If more sensitive technical material needs to be provided, please first send a description of the material and wait for further instructions.

4. INFORMATION TO INCLUDE

A report should include at least the following information:

i) the type number from the device nameplate; this information is mandatory where the report concerns a specific device or machine;

j) the serial or production number of the device, if available;

k) the name of the product, machine, software, or affected component;

l) the firmware, software, operating system, or configuration version;

m) a concise and factual description of the vulnerability;

n) the potential impact on confidentiality, integrity, availability, machinery functionality, or the safety of persons;

o) steps that allow the issue to be reproduced or verified;

p) proof-of-concept code, screenshots, a photograph of the nameplate, relevant log extracts, or other supporting material, if available;

q) whether the vulnerability is publicly known, has been disclosed to another person, or shows signs of active exploitation;

r) the date and approximate time of discovery;

s) the reporter's contact details for follow-up communication.

The report should contain only the information necessary to identify, assess, and remediate the vulnerability. Personal data and third-party operational data should be removed or anonymised wherever possible.

5. RULES FOR SAFE TESTING

A reporter may perform testing only:

- **t)** on a device they own; or
- **u)** on a device, system, or licence for which they have prior demonstrable written authorisation from the owner and, where applicable, the operator.

Testing must be proportionate, cautious, and limited to what is necessary to confirm the existence of the vulnerability.

The following activities are prohibited:

- **v)** testing machinery or systems in active production without the prior written consent of the owner and operator;
- **w)** disabling, modifying, bypassing, or testing the limits of safety functions, protective devices, emergency stops, or control functions in a way that could endanger people or property;
- **x)** causing downtime, reducing availability, flooding a service, damaging equipment, or losing or modifying data;
- **y)** obtaining, downloading, copying, modifying, or disclosing data beyond the minimum necessary to confirm the vulnerability;
- **z)** accessing third-party accounts, data, or systems;
- **aa)** social engineering, phishing, physical intrusion, fraudulent conduct, or contacting employees outside the security contact;
- **bb)** using a vulnerability to gain an advantage or financial benefit, to extort, or to demand a reward;
- **cc)** installing malicious code, maintaining hidden access, or further distributing the vulnerability;
- **dd)** disclosing technical details before the case has been coordinated.

If testing could affect machinery functional safety, testing must stop and the finding must be reported without delay. Further verification may only take place in a safe, isolated environment and with appropriate authorisation.[3]

6. REPORT HANDLING AND COMMUNICATION TIMEFRAMES

HQ Systems s.r.o. will aim to:

- **ee)** acknowledge receipt of a report within 7 calendar days;

[3]Nařízení (EU) 2023/1230 o strojních zařízeních: https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng

ff) perform an initial assessment and provide the reporter with a preliminary response within 30 calendar days after receiving a sufficiently complete report;

gg) provide a further status update for an open case at least once every 60 calendar days, where permitted by the nature of the case, contractual and legal obligations, and the protection of sensitive information.

These are target communication timeframes and are not a guarantee that the vulnerability will be fully remediated within those periods. The start or running of a timeframe may be affected by an incomplete report, the need for additional information, unavailability of the device, coordination with an OEM customer or supplier, testing complexity, functional safety requirements, or legal restrictions.

HQ Systems s.r.o. will prioritise a report according to the severity and likelihood of exploitation, impact on the safety of persons and operations, the range of affected products, the availability of mitigating measures, and any indication of active exploitation.

A report involving an actively exploited vulnerability, a severe security incident, or an imminent risk to people or operations may be handled on an accelerated basis. The voluntary communication timeframes in this policy do not extend or replace any shorter period imposed by law for reporting to competent authorities.

7. REMEDIATION AND COORDINATED DISCLOSURE

The method and schedule for remediation will be determined individually, taking into account risk, technical complexity, functional safety, available mitigations, validation of changes, distribution of updates, contractual responsibilities, and any required coordination with an OEM customer or component supplier.

This policy does not establish an automatic fixed deadline for public disclosure. The date and scope of disclosure will be determined case by case, particularly in light of:

hh) the severity and impact of the vulnerability;

ii) the existence of active exploitation;

jj) the availability of a fix or effective mitigation;

kk) the time needed to verify, validate, and safely deploy remediation;

ll) the risk that premature disclosure would increase risks to users or the safety of persons;

mm) statutory reporting and information obligations;

nn) the legitimate interests of an affected OEM customer, operator, or supplier.

The reporter is requested not to disclose the vulnerability or its technical details without prior written coordination with HQ Systems s.r.o.

HQ Systems s.r.o. may delay disclosure where the security risks of disclosure outweigh its benefits, particularly until affected users have had a reasonable opportunity to apply an available fix or mitigation.

Where a security update or other corrective measure is released, HQ Systems s.r.o. will provide affected users with information to the extent and at the time required by applicable legal, safety, and contractual requirements.

8. INFORMATION SHARING AND PROTECTION OF IDENTITY

To the extent necessary, HQ Systems s.r.o. may share technical information from a report with:

- **oo)** the affected OEM customer or operator;
- **pp)** the manufacturer or supplier of an affected component;
- **qq)** professional advisers involved in verification or remediation;
- **rr)** the competent CSIRT, ENISA, or another competent authority;
- **ss)** another party where necessary to remediate the vulnerability, protect persons, perform a contractual obligation, or comply with applicable law.

The identity and direct contact details of the reporter will not be disclosed to third parties without the reporter's prior consent, unless disclosure is required by law, an order of a competent authority, or the need to protect against a serious and imminent threat.

Where the case can be resolved without sharing the reporter's identity, only the necessary technical information will be shared with third parties. This does not restrict the processing, retention, or disclosure of information required by law.

9. ACKNOWLEDGEMENT, REWARDS, AND LEGAL STATUS

HQ Systems s.r.o. may thank the reporter for a proper and useful report. This policy does not create any entitlement to a financial or other reward, public attribution, employment, a contract, or any other consideration.

HQ Systems s.r.o. does not currently operate a bug bounty programme.

This policy does not constitute general authorisation to access devices, systems, or data belonging to HQ Systems s.r.o., its customers, or third parties. It also does not constitute a promise that HQ Systems s.r.o. will refrain from exercising its rights where conduct exceeds the rules of this policy, causes damage, endangers people or operations, breaches a contract or applicable law, or interferes with third-party rights.

10. REGULATORY REPORTING

HQ Systems s.r.o. may be required to report an actively exploited vulnerability, a severe incident, or other relevant facts to a competent CSIRT, ENISA, a market surveillance authority, a customer, or another party within a period specified by law or contract.[4]

The 7, 30, and 60-day timeframes in this policy apply to communication with the reporter. They do not restrict, extend, or replace statutory reporting deadlines, the duty to address vulnerabilities

[4]Regulation (EU) 2023/1230 on machinery: https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng

without delay, or the duty to take measures necessary to protect people, products, systems, and data.

11. POLICY UPDATES AND PREVAILING LANGUAGE

HQ Systems s.r.o. may update this policy, particularly in response to changes in law, products, contractual relationships, technical capabilities, or internal processes. The current version will be published on the HQ Systems s.r.o. website.

In the event of any discrepancy between the Czech and English versions, the Czech version shall prevail.

REGULATORNÍ REFERENCE / REGULATORY REFERENCES

1. Nařízení Evropského parlamentu a Rady (EU) 2024/2847, Cyber Resilience Act, zejména články 13 a 14 a přílohy I, II a VII https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02024R2847-20241120

2. Nařízení Evropského parlamentu a Rady (EU) 2023/1230 o strojních zařízeních, zejména příloha III, body 1.1.9 a 1.2.1 https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng