JCB Vulnerability Disclosure Policy

Version	3.0 DRAFT
Effective date	
Policy owner	JCB Information Security
Corporate IT / digital services contact	security-report@jcb.com
Product Cybersecurity contact	psirt@jcb.com
Ref	JCB-ITP002 / JCB-GRP-232

1. Introduction

1.1 The purpose of this policy is to set out rules for responsible and coordinated disclosure of potential security vulnerabilities affecting JCB. JCB wants to work positively with the security research community, customers, suppliers and other stakeholders to improve the cybersecurity of JCB information systems, digital services and products with digital elements.

1.2 JCB supports and appreciates the work done by ethical security researchers in identifying and responsibly reporting potential vulnerabilities. JCB is committed to working with reporters in good faith to verify, reproduce and respond to legitimate reported vulnerabilities in a timely and responsible manner.

1.3 Reported vulnerabilities will be reviewed by the appropriate JCB team. Reports relating to corporate IT systems, websites or digital services will be reviewed by JCB Information Security. Reports relating to products with digital elements, embedded software, firmware, connected functions, service tools or diagnostic tools will be routed to JCB Product Cybersecurity / Product Security Incident Response Team (PSIRT) as appropriate.

2. Scope

2.1 This policy applies to third parties reporting potential cybersecurity vulnerabilities to JCB. Third parties include any person or entity who is not employed by JCB or directly contracted by JCB to provide the relevant service or testing activity.

2.2 This policy applies to vulnerability reports relating to:

2.2.1 JCB corporate IT systems, websites, digital services and web or mobile applications;

2.2.2 JCB products with digital elements, including connected machines, embedded software, firmware, ECUs, machine control systems, telematics systems and connected functions;

2.2.3 JCB service tools, diagnostic tools, update mechanisms, software distribution channels and supporting cloud services;

2.2.4 JCB product cybersecurity interfaces involving suppliers, open-source components, customers or other manufacturers, where the report may affect JCB products, services or users.

2.3 This policy does not authorise testing that would cause harm, create a safety risk, disrupt services, compromise data, breach the law, or interfere with customer, dealer, supplier or JCB operations.

2.4 Reporters should read this policy before submitting a vulnerability report to ensure the requirements are understood and any disclosure is made in accordance with this policy.

2.5 JCB will publish the security.txt document on the JCB website under the /.well-known/ path. See Appendix A.

3. Reporting channels

Reporting route	Contact	Use for
Corporate IT / digital services security	security-report@jcb.com	JCB corporate IT systems, websites, web or mobile applications, digital services and information security issues.
JCB Product Cybersecurity / PSIRT	psirt@jcb.com	JCB products with digital elements, embedded software, firmware, ECUs, connected machines, service tools, diagnostic tools and product cybersecurity issues.

3.1 If a reporter is unsure which route to use, either contact route may be used. JCB will internally route the report to the appropriate team where necessary.

3.2 These reporting routes are for vulnerability reports only. They are not intended for technical support, customer support or general product enquiries.

4. Responsibilities of reporters

4.1 JCB expects any person carrying out vulnerability testing or research to act responsibly and in good faith. Reporters should:

4.1.1 Make reasonable efforts to avoid privacy violations, destruction of data, service disruption, safety risk, machine disruption or degradation of systems or services;

4.1.2 Report suspected vulnerabilities to JCB using the reporting channels in this policy before making any information public;

4.1.3 Provide only the information necessary to demonstrate and allow assessment of the suspected vulnerability;

4.1.4 Securely delete any data obtained during research as soon as it is no longer required and, in any event, no later than one month after the vulnerability has been resolved or JCB confirms the data is no longer required;

4.1.5 Follow the coordinated disclosure expectations in this policy before making any vulnerability information public.

4.2 JCB does not encourage active vulnerability hunting. Any testing must remain limited, reasonable, authorised and necessary to understand or report a suspected vulnerability.

5. Activities not authorised by this policy

5.1 This policy does not authorise any activity that is unlawful, unsafe, disruptive, destructive, or outside the scope of reasonable good-faith vulnerability reporting. Reporters must not:

5.1.1 Access, modify, delete, exfiltrate or attempt to access data, accounts, products, systems or services that do not belong to them or for which they do not have express authorisation;
5.1.2 Publicly disclose vulnerability details without JCB's prior written agreement or without following an agreed coordinated disclosure approach;
5.1.3 Send unsolicited mail, spam, phishing messages or other unsolicited communications;
5.1.4 Upload, transmit, post, link to, send or store malware, viruses, trojans, ransomware, backdoors or similar harmful software;
5.1.5 Conduct denial-of-service, distributed denial-of-service, volumetric or resource-exhaustion testing;
5.1.6 Conduct social engineering, phishing, physical intrusion, tailgating or similar testing against JCB employees, contractors, dealers, customers or partners;
5.1.7 Carry out product vulnerability testing on customer-owned machines, live worksites, public environments, safety-critical operating conditions or machines, products or systems not owned or authorised by the reporter;
5.1.8 Access unnecessary or excessive amounts of data. Reporters should use the minimum information needed to demonstrate the suspected vulnerability;
5.1.9 Create risk to people, property, machine operation, customers, dealers, connected services, data, finance systems or JCB operations;
5.1.10 Share, redistribute or fail to properly secure any data obtained during testing or research;
5.1.11 Attempt to bypass sanctions, export control, legal or contractual restrictions.

5.2 Findings derived from physical testing, office access, social engineering or similar activities may be passed to the appropriate JCB team, but those activities are not authorised by this policy.

5.3 Only original vulnerabilities that are previously unreported and not already known to JCB are in scope for handling under this policy.

5.4 Benign user interface issues, spelling mistakes and general technical or customer support enquiries are outside the scope of this policy. TLS configuration weaknesses and services hosted or operated solely by third-party providers may also be outside scope unless they present a material risk to JCB systems, products, services or users.

5.5 JCB may reject or close reports that appear to be automatically generated, bulk-submitted, speculative, unsupported by meaningful evidence, or produced primarily by automated or artificial intelligence tools without independent validation by the reporter.

6. Information to be included in a report

6.1. The initial report should include enough information for JCB to understand, triage and route the potential vulnerability. Where possible, reports should include:

6.1.1 Reporter name and contact details, unless the reporter wishes to remain anonymous;

6.1.2 A summary of the vulnerability, potential exploitability and potential impact;

6.1.3 The affected product, system, service, website, application, component or tool;

6.1.4 For corporate IT or digital service reports: URL, IP address where relevant, application name, browser, operating system, mobile platform, app version, device model and testing environment;

6.1.5 For product cybersecurity reports: product name, machine model, serial number or range if known, system/component name, ECU, software or firmware version, service tool or diagnostic tool version, supplier or component reference if known, and any available product context;

6.1.6 Steps to reproduce the issue, provided at a level appropriate for initial triage and without including sensitive exploit details in the first contact;

6.1.7 Any available evidence of active exploitation, compromise indicators, safety impact, customer impact or operational impact;

6.1.8 Suggested remediation or mitigation information, if known.

6.2 Sensitive technical details, proof-of-concept exploit material, personal data, confidential information, credentials, cryptographic keys or customer data should not be included in the first contact. JCB will provide secure communication instructions where required.

6.3 Reporter names and contact details are optional. Where provided, JCB will use those details only to communicate with the reporter about the reported vulnerability, unless another use is agreed or required by law.

7. Acknowledgement and handling

7.1 JCB aims to acknowledge receipt of in-scope vulnerability reports within 7 calendar days where valid contact details are provided. Where we receive reports that are in breach of section 5 of this policy, we reserve the right not to acknowledge receipt of the report.

7.2 An acknowledgement does not confirm that the report is valid, exploitable or applicable to a JCB product, system or service.

7.3 JCB will assess the report and may contact the reporter for clarification, additional information or secure transfer of sensitive technical details. A dedicated JCB contact may be assigned where appropriate.

7.4 Validated reports will be recorded and managed through the appropriate JCB vulnerability management, incident response, remediation or JCB Product Cybersecurity / PSIRT process, including relevant supporting standards where applicable.

8. Coordinated vulnerability disclosure

8.1 JCB supports coordinated vulnerability disclosure. Reporters are expected not to disclose vulnerability details publicly until an agreed disclosure approach has been established or the vulnerability has been remediated or mitigated and disclosure no longer presents an unacceptable risk.

8.2 Where a reported vulnerability affects JCB products, suppliers, open-source components, customers, users, dealers, other manufacturers or other stakeholders, JCB may coordinate with relevant parties before public disclosure. This coordination may include assessment, remediation, mitigation, advisory preparation, customer communication, regulatory assessment or other appropriate action.

8.3 The timing and content of any public disclosure will depend on the vulnerability, affected product or service, remediation status, operational risk, safety considerations, customer impact, legal obligations and the need to avoid increasing the risk of exploitation.

9. Secure communication

9.1 Vulnerability information can be sensitive. Where sensitive technical details are required after initial triage, JCB will provide instructions for an agreed secure communication route.

9.2 JCB may request that additional technical details are submitted through an agreed secure communication route. JCB Information Security and JCB Product Cybersecurity / PSIRT should review and maintain the secure communication mechanism used for vulnerability reports, including any relevant security.txt encryption reference.

10. Remediation, mitigation and advisories

10.1 JCB will assess validated vulnerabilities and determine appropriate remediation, mitigation, risk treatment or communication. The priority for fixes, mitigations or communications will be based on severity, exploitability, affected product or service context, customer impact, safety considerations, technical feasibility and complexity of execution.

10.2 Where JCB publishes product security advisories or user communications, these may include affected product identification, potential impact, severity, remediation or mitigation guidance, release date and update information, as appropriate to the vulnerability and disclosure context.

10.3 JCB may work with the reporter, suppliers, customers or other stakeholders to confirm that a remediation or mitigation adequately addresses the vulnerability where appropriate.

10.4 Where remediation cannot be completed within an applicable target timeframe, JCB will document the reason for delay, any interim mitigation and the revised target date.

10.5 Where appropriate, JCB may confirm when a reported vulnerability has been resolved, mitigated or otherwise closed.

11. Incident escalation and regulatory reporting

11.1 Where a reported vulnerability is suspected or confirmed to have been exploited, is associated with indicators of compromise, or may have resulted in unauthorised access, data exposure, service disruption, safety impact or other material security impact, JCB will assess whether escalation to the appropriate incident response, JCB Product Cybersecurity / PSIRT, legal, regulatory or customer communication process is required.

11.2 Where a product cybersecurity report may be relevant to JCB's obligations under applicable laws or regulations, including cybersecurity reporting obligations for products with digital elements, JCB Product Cybersecurity / PSIRT, Information Security, Legal and relevant business owners will coordinate the internal assessment and any necessary regulatory reporting route.

12. Legal requirements and good-faith reporting

12.1 This policy is designed to be compatible with good-faith security research and responsible vulnerability disclosure. It does not give permission to act in any manner that is inconsistent with the law or that causes JCB to breach legal, contractual, privacy, safety, export control or regulatory obligations.

12.2 Relevant legal obligations may include, but are not limited to, the Computer Misuse Act 1990, the General Data Protection Regulation 2016/679, the Data Protection Act 2018, and the Copyright, Designs and Patents Act 1988.

12.3 JCB will not seek punitive action, such as suspending or terminating accounts, or legal prosecution, against a security researcher who reports, in good faith and in accordance with this policy, a security vulnerability on an in-scope JCB product, system or service. This statement does not apply to activity that is unlawful, harmful, unsafe, disruptive, extortionate, malicious, negligent or outside the scope of this policy.

12.4 JCB does not operate a bug bounty or reward programme under this policy. Submission of a vulnerability report does not create any entitlement to payment, compensation, reward, employment, contract, or other benefit.

13. Feedback and continuous improvement

13.1 JCB may invite reporters to provide feedback on the vulnerability disclosure process. Feedback will be used to improve JCB's vulnerability handling, disclosure, communication and remediation processes.

13.2 This policy may evolve over time to remain clear, complete and relevant to JCB products, services, regulatory obligations and cybersecurity good practice.

Appendix A

This appendix provides the proposed security.txt content. If JCB has or creates a dedicated secure submission portal, PGP key or S/MIME secure mail page, an Encryption field should be included to link directly to that mechanism.

```
https://www.jcb.com/.well-known/security.txt

# JCB vulnerability disclosure contacts

# Product Cybersecurity / Product Security Incident Response
Contact: mailto:psirt@jcb.com

# Corporate IT / digital services security
Contact: mailto:security-report@jcb.com

# Vulnerability Disclosure Policy
Policy: https://www.jcb.com/en-GB/explore/corporate/

Preferred-Languages: en

# Do not include sensitive technical details, proof-of-concept exploit
material, personal data or confidential information in the first
contact.

# JCB will provide secure communication instructions where required.

Expires: 2027-12-31T23:59:59.000Z
```