Version Date: 2026-06-03
Version #: 002.5

KORELOGIC - PUBLIC VULNERABILITY DISCLOSURE POLICY

This document addresses KoreLogic’s policy, controls, and organizational responsibilities associated with its Vulnerability Disclosure Program. Specifically, this document defines KoreLogic’s vulnerability disclosure policy, process and guidelines to product vendors, security vendors, and the general public.

Scope

During the course of our practice as security researchers, KoreLogic may discover novel vulnerabilities in public software and hardware products released and/or sold by a person, group, organization, or company (Vendor). The purpose of KoreLogic’s Vulnerability Disclosure Program is to responsibly distribute vulnerability information to the public in a controlled manner and follow common industry practices associated with disclosing newly identified vulnerabilities, which are not protected by KoreLogic client confidentiality/non-disclosure agreements.

Policy

Based on Scope defined above, the following policies will guide KoreLogic’s Vulnerability Disclosure Program:

KoreLogic will responsibly notify the appropriate product Vendor of a security vulnerability with their product(s) or service(s).

Regardless of Vendor acceptance or validation of the vulnerability, KoreLogic will release the vulnerability to the public upon completion of the steps defined in the Disclosure Controls / Process Section documented below. The standard disclosure deadline will be forty-five (45) business days after initial Vendor contact.

All decisions regarding final public release status are made at the discretion of KoreLogic’s Vulnerability Disclosure Review Board. Unless there are exceptional circumstances where this body has determined a delayed public release period is warranted, KoreLogic will follow the standard disclosure process.

KoreLogic will make every effort to work with the Vendor to ensure they understand the technical details and severity of a reported security vulnerability. If a Vendor is unable to, or chooses not to, patch a particular security flaw, KoreLogic, where possible, will offer to work with that Vendor to publicly disclose the flaw with an effective workaround. In no case, however, will a vulnerability disclosure be suppressed as a result of Vendor intervention.

KoreLogic will not release vulnerability information without first attempting to contact the Vendor. KoreLogic will internally vet any vulnerability and/or remediation information that it provides to the Vendor.

Communication between KoreLogic and the Vendor regarding vulnerability notification may be published publicly once the vulnerability itself has become public. Vendors will be apprised of any publication plans, and alternate publication schedules may be negotiated at the discretion of the KoreLogic Vulnerability Disclosure Review Board.

In cases where the Vendor is unresponsive, or will not establish a reasonable time frame for remediation, KoreLogic may disclose vulnerabilities fifteen (15) business days after the initial

contact is made, regardless of the existence or availability of patches or workarounds. The final determination of the type and schedule of publication will be based on the best interests of the community overall.

Disclosure Controls / Process

KoreLogic will utilize the following controls and processes to guide KoreLogic's Vulnerability Disclosure Program:

1. Vulnerabilities disclosed during KoreLogic's disclosure process have been identified by our security engineers and analyzed by our Vulnerabilities Disclosure Review Board.

2. Upon discovery of a new vulnerability, KoreLogic will verify, using various open-source vulnerability databases, that the vulnerability has not been previously disclosed.

3. Upon identification of a security vulnerability, KoreLogic's first attempt at contact will be through any appropriate contacts or formal mechanisms listed on the Vendor's Web site, or by sending an e-mail to the appropriate security point of contact (e.g., security@, support@, info@, secure@vendor.com, etc.) with the pertinent information about the vulnerability. KoreLogic will not submit vulnerability information via online forms. However, online forms may be used to request the Vendor's security point of contact information. KoreLogic will PGP-encrypt all emails exchanged with the Vendor if the Vendor supports PGP and can provide a public key. During this initial e-mail notification, KoreLogic will indicate its plan to disclose the vulnerability according to a specific timeline. The Vendor is encouraged to reply to the initial e-mail and work with KoreLogic to determine a solution timeline.

4. Simultaneous with the Vendor being notified, KoreLogic may distribute vulnerability protection updates for the purpose of detecting and/or remediating this vulnerability to any or all of its clients who may be affected.

5. If the Vendor fails to acknowledge KoreLogic's initial notification within five (5) business days, KoreLogic will initiate a second formal contact to a representative for that Vendor. If the Vendor fails to respond after an additional five (5) business days following the second notification, KoreLogic may rely on an intermediary to try to establish contact with the Vendor. If KoreLogic exhausts all reasonable means in order to contact the Vendor, then KoreLogic may issue a public advisory disclosing its findings fifteen (15) business days after the initial contact.

6. KoreLogic reserves the right and may notify Carnegie Mellon's Computer Emergency Response Team (CERT) or US-CERT, whether or not the product Vendor has responded to KoreLogic.

7. KoreLogic realizes some issues may take longer than the allotted time due to mitigating factors, and we are willing to work with Vendors on a case-by-case basis to resolve the matter in a reasonable time frame. If the Vendor is not responsive, unable, or unwilling to provide a reasonable statement as to why the vulnerability is not fixed within the allotted time frame, KoreLogic, with or without any additional notice, may publish a public advisory to inform the defensive community. KoreLogic expects Vendors who have requested extra time to proactively provide periodic, but not less than monthly, status updates on their remediation progress. If an expected update is not provided, KoreLogic will make up to three (3) attempts to solicit one and if no

update is provided after that KoreLogic, with or without any additional notice, may publish a public advisory to inform the defensive community.

Organization Responsibilities

KoreLogic maintains a right to the following:

KoreLogic may produce and provide a timeline for release and notification as outlined in Step 3 above. The initial e-mail will also provide the Vendor with information about the vulnerability, scope of vulnerability, disclosure timeline, and other useful information for reproducing the issue where feasible. In cases where Proof-Of-Concept (POC) exploit code is available, KoreLogic will provide and securely transmit such information only upon request to the Vendor. This includes all code and information required to allow the Vendor to verify the vulnerability and develop an appropriate solution.

Public disclosure may include the release of the vulnerability details on the KoreLogic web site. KoreLogic may also release the vulnerability details through industry standard media avenues at its own discretion or that of the Vulnerabilities Disclosure Review Board.

KoreLogic may deem it necessary to release the vulnerability details before the initially planned or policy controls release schedule. Extenuating circumstances or situations that require changes to an established schedule may include but are not limited to the following:

Highly active exploitation

Threats of an especially serious nature, including but not limited to:

Potential impact to critical infrastructure

Possible threat to public health and/or safety

Vendor releases a patch and acknowledges the vulnerability publicly in advance of the indicated timeline

Wide-spread exploitation of the vulnerability is evident

Publication of details of the same vulnerability by a third party, such as by independent discovery

Media coverage about the vulnerability exposes the vulnerability to the public

Immediate mitigations are available

Policy Management

KoreLogic updates its policies, processes, and procedures on a regular basis. KoreLogic reserves the right to modify the policies, controls, process and its responsibilities associated with its Vulnerability Disclosure Program without notice to Vendors or public. Vendors are encouraged to contact KoreLogic should clarification of the disclosure policy be required.

For specific questions, please send inquires to the following email address:
disclosures@korelogic.com

The fingerprint for the PGP key associated with this address is:

6845 509C 3270 0028 FA34 A901 0280 4A51 F572 7BBC

And the full public key, also available at
https://korelogic.com/pgp/disclosures_korelogic_02804A51F5727BBC.asc, is:

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGm9SOwBEADVqCzDhTN/E6RhvIu4wAIMRjFkgyF8JOybSI0Kn/I1YtElcKDE
AOiAzeFIpsZcgCWc7gTUoiNLSnnwIspcH//ox7JdArAn9hPi35M2vxnM4OLxJX4N
V6komtk48T4nTT6e3KjJtWgFeUHxRL+M48looZ8PKdK6oZiBKYzJSQZH09nJlT9J
oUXvLnUSH/0Bwz9dhaYcBVBp/hr8xbSt6cJmfX3wfRisfxJ7WE0qYHe+7G57qQ52
FaqLECz7VMJXH0vrP+4x5p5l+FUR4uNOfCab7afgf1MKm2MU1qmhpq8AfEjwuief
6pFCjpW9JMZkIo+jsQcKVW4Rv/UFQ3bHvdhxv2RUsQ8X0bFSeLlubsl+Odo67pFR
45AiMuz3RqryPSgFFPYs3gHTcMCpX0KpSvFplLNrYFJRzm7/21CI9PAQBoZGQb8d
nQ4rLvOJywbUOXl9YV2XYfvAt+TSjU53HHoqYv19RblhVr5xntTe3nY6kI1XiL+n
IcZugJ3FiufBrmpJYhM7kOfnY+PkGE1/TA8rftkkP4NMQgZPphh3kkQDJ1lLillO
d/csdvLbMzfAxBfB6NoUkdseGTJKMZ+BjnPBnH2BnGxG07dFr8r8wFzG0UO2uTdz
fKsL95gpxg825H2RZRBPp1a1itzzDHNe+8mqcPvixosJtMb3dTqOJYdeEwARAQAB
tFVLb3JlTG9naWMgRGlzY2xvc3VyZXMgU2lnbmluZyBLZXkgKFNpZ25pbmcgS2V5
IDIwMjYtMjAzMCkgPGRpc2Nsb3N1cmVzQGtvcmVsb2dpYy5jb20+iQJUBBMBCAA+
FiEEaEVQnDJwACj6NKkBAoBKUfVye7wFAmm9SOwCGwMFCQeEzgAFCwkIBwIGFQoJ
CAsCBBYCAwECHgECF4AACgkQAoBKUfVye7wf0hAAliIXF2PKe5S3nyBWLENjPa3n
hGGrowmeq5xVQwrt4c9NrFdaLtzLN3et7CyCNpgGZWSCAD7zUQZ5VfhhhSDTye69
WU4UHha7wZcJeAn1Bs8htYCOkQQZUugxZrPmidmYcsduxwmgvZ3YKxo30TQmr2LG
e6X0Atl+h3jUBUGshjuZz2Iln3yEj8B2JaUCWtmUI+jCPGV5ElyqwD2IV+HJ4ruW
++OWDpqdmKTD6pFHiQIp8svw5JjgPhOJrJ4Bk+mWRkNJx+Gl+8/eGiVPUwg2BzEV
yeRPlpnHSuBlFLiKzEQgHCxqINAGcwjx8xkA2eBobK97NFL1cMOFDJRzmiFn2Dc/
gwSehKylj5fojyxaBnYyKGXw4YVWPw3RVK+GVlYwzoIkslsbMhdDBMz2JyC7u5u+
yFjMwwvDxsMzmuEGEgJ9nLPN6VR+z7HnAkyXs6t0/oz3klQeAqRUXwDX/V4IrMuL
LOpbT8Xp+itRMQ1jp8WaU3NHyE76iDC9quKKRDgpFOHw8xIPkDnPvTObz9ppsMr9
0au0w7adGhROATPkVdrw+46wiE02lli6ObErudyUmNUX58i6tZ/NcJT7DwwoG38z
pu1KdlDGztrYp4f+v6mAWsrbjvFYX36TsQgDqIcWCa4h51jvHTHwJ32H6xuwvA6B
rBUIRthTr1uz7ujyYeGJAjMEEAEIAB0WIQQHXZZhnBtXBhMn9vYMouwJOVaR6QUC
ack69gAKCRAMouwJOVaR6TSGEACcu7kngSzUMSD5UzLqjHj+NfJFCo/zetyquyRM
rPJlpf4iN+ARiZweq8or/aAPAIORwPoNV/ebQ9QtCdR5yiq+GzljOQwvIwV4KCaQ
jKctbVQWhHxXlx5H/1dSdVgF4hXljp8DojaXftOKhqiBNG1a/SisZVUXDt2tF3j0
M8bLWgkzJ9hB4SJVnYV+fS0flsukLoQAtQsbQo3uyn28UMTWgIpRbwdW7U05/qgM
Fc85ul6DzJ0E3N6DpSZy0oChjnBjx5LTxvc15wyZXkxl4QNHrFflmyAcJ/XXItGm
ao4XSYaV9QLOLKyNNzwn9Wu8/XsyZ8Jf0tBpAOJ6gGuOqdimyWOc0hf8CJOoriV2
8PZEq3oQV5ckJdgRSp28Vuv//3x2ISE97sS5hjO6YzMaV90Q9vymsQ7x5p0BD26e
Z1Uefli4MASL4UZws2PGqcOmcvUyXYwGSUD7HmKrLoYfeARCVnxH878cdTiJ1nse
yL5vQuVPpm47q8JPAkOgZq+BoSlQiHL6PPWWGDaget67nbZHfyrbBoGl/PsERBBD
+Juddo2VUBpmfFWhu2XmmiEN5WPSZs68kvbOJRq4vMOdD1ObMUK56tAZsX/AS609
sLZbmDFh1+O8+Cyowfr7OZfYKbHvsa0a2C/+RvCyZW+XZ4Qqwnj0iTgj39+gs5rH
QfUXlYkCMwQQAQgAHRYhBFMUxnEUvYQK98wxuKkTOQABI3YDBQJpyUFjAAoJEKkT
OQABI3YDuGQP/0/xDOT/zphbo485Xtmj4KdAasyYxbHqXwOdd2bjTzyHxLVDusq2
gYebfvMpd63JxxE0TxXn5DdvHuj217+hZ7pa9bxMp+X7WZX1+vk7jPufd76uMLw5
nuBpzJlgePiGe1gJHw8a5I8UThMeAo4AXqwrFJ9ayBetCr8fimGL+BZXLPcnfUup
GGzyjUxt8xg5Zvq8iZxwsuKSmN2DerUrd1NO5Pjj/ACrvS9/Hn7ZQ19ikPeiIGR9
SMtv6v3NO6Y9KSqFubCiGt/1R2uNLDgdtGwuoCtb1xZcoY5PELLXBVoek3Nj9RUo
D0Inn+J3n806OsZfvXDodrIYw/4xl2dg4nfZ9DGdd1bHwhrLTV0P6djXtHvx+Lob
Jbo9Z5Qm6f6r4pqrl1Et5gFYr8z2TYj3ny15DQqONKZ3da5v677u9CORWvZId7Gj
SgzoMOyFBqyN5aqKIilpVlPMTPTR4ngN9wb8sTjjC7riwxCxlp92bK6YxNaHtQph
S/Y+4H9rrmDB3pGnPhPdlYqcTwjk7bv7N5de+H9MeoMFIgKUhB9xZp2nf/iHoab/
uG/ZWVXDBT9B3RyCM6Tryuk/lMIB2XxZXoChms3R4/sBZKs8Cirq6aE833yf1Jw8
cwgN5DnUMswc1HP2VsHXckjYW2c2ye1Hv4gIbpBTZuJHJg7sDqC7KANwiQIzBBAB
CAAdFiEEhCjtFFJoxycMSPRUhG8GN1/rFhIFAmnw1pwACgkQhG8GN1/rFhKuURAA
gZ/Gy66E9VUW8cLLFhNoWFMz0JsVlER7/mjeg5NKDhhEr9zpm8Mrif6Y7w6xoZoW
NBpEOMcdAUGFrCfx+zrL3okZ6iH7nMOxOeDZvOSMWrp/SGyQDtl/sQpCO72HurLQ
Zc6C0mcZ4ZNjhcPhxjiTWElNSalWmp8aj0rolgTO9j3TdV1SsswD31MMqQzvj0y2
7FIvTv9LrX4Mfk/ADlQBsTOpzgp7IdymGbBVVUl0Ae1HS4IuRQhzCskJg6leWLsJ
wakEmSmD4CCft8OkRKW8ptDAT9hbSVv6qw8DYXSDJZjrRLuM2stKEUkYMRtTXJ8v
nQ42ep2d7b1I23OeHGoyubo55i1exLCP5j7JM57IThbaQykke5RfdT/O9Um/1RUA
qZBjrcS5eLqWhTXocsPdyiEUG1i+R/KHWCUqlut2KNOea9z2GG+l3fUUq9TOOAjA
OrtXc7TeXZRqLThFMAGUCE3jqh+4q/76RKttLleNzLRUw4yE4XZbzdr/aiyqurYM
vlYidIOmiD+6YZCtrLWQc6tSWRxTDlPV3/jxdoDNlKDtJSGV7GK6Vwfx6ZyW2LOO
UMxIETJgaMjHYga/zVja/uxfnFa0SPAY/XG+2YPoWsnd4thSwebcqVvEAP5TQ9/f
WVhIBiA3rT3ayqB3DWr5g9laDbbRqmglY2nkd9fY9HiJAjMEEAEIAB0WIQQdGJYt

```
wu+kYFnYaAXuF7KuPBZW/QUCahh2WQAKCRDuF7KuPBZW/WX6EACiTqr0U+XzFZ2D
u0FKsTzFw9AuO9p53dBCIIOSxJqy0v31EWeQeFPUWTXY9T//zRnQRXgw5nzWODU7
DkqldKsF6eC7IvfYkZGcnY5h+1s/7Ul2znK+9pkYxv4rv2LfTrV29NWLmp7XxqQc
JCqmdZn3YaqiiStFGQ9rKg4JtQy3O1rACr5PTQP7CR6/SirAD9SrtsRMs95Lbgjx
DmxcajuBXdgNr8xW9Xqgj5Zb1rgZp6eTWveoFY10bJr6a6WZKpJzBLXvB0EbTYS7
ZwKsHzi5Goh6BsHM/bHa7mZHUJ+UOcEu/p8PvWWhCTXrE7AzDOR++YNIGKM0PilX
fu7Td+n7ZgEIlE1twiY73Ce4Hl9P0diTPVE/wcGdgNbqeBn/zqWsXWUjcrXFVc73
4O0hhuwIxPHg9vGWbwAqN5OTd2P7bKwskunx4kOKwjKB6n4lIKfriVqw2gN02ziT
x0m3xF4zHEYlyKQplWh3zBQvS3VDXrjasbwGX8MBTHFeiz2jtneP3+Mv2UjslqIR
2OBSqVXI5VP4KkgdfSeY+JoUkgRGoonivOpVWACQZKLQWFrRm6n+NRNi6BsU3aT3
epGpTy643tfyVq73HL1tN3Lxoag9ffvf+j3uWcOgNB8ar1lWVCGx1Z7l3YuUJbYf
B6+T8bWgvqbpjGXeIcm9+cX3ILF75LkCDQRpvUjsARAAocJDSxj3YJn7iPHE6ja2
c1CALRB8gr/iKGYn1klyw/WUkfAp1/ilAxNI8IebKvl3SXLP8DbH56DgNMPhjXBe
3N6awcf5xDrJQPzZSbQ4e/g3blp/UE6M6AOXDhVkX4kHL5h1tsAwZ6Eb11q9HL0S
a1H2J4BJaPlrB9tZ5YKa7HPpYycUteJAiToNDGss8g+PwvILyvCeJ6eL185d5dNV
SEYoepaf/fPWnq3aNusofNqZwI8lr3vC5KCLPLKCEiGGYNf47iv4OLJoVdyWR66f
hRpueivB7Hr+Hevush9s5VXlMzptL2SYv6w6npa7nH4dYOcP81b2kXCFwj+QLzET
TTCd3bFg9kFNyZXq6cJlzJWra9mMTNpztiTNO7ge9+gqzLVZsyAK2hl9EzY1QSHn
Hp610lUTKx3vJzVayfpsvyEtOcdsXidhhwrTgslFfFMeAlyYU1DhzYk++VIrKzrh
vUrNKj+q4pEP13UA1SewCCdgKtfODxJ/lSYItHvQYE8v4fJ0Vl4U5/ppYcGVmzUX
BH33qTRwGX9n0PKLKUbz79qVVNIyYW/xq5WKtEhvBhh3iSoChrQ6lW30bc/rGsmB
9Lq5+4+kLNOi1sa9fF2/URlL7t64PKZ3AReAZkEd1YnArS6ESL8iTzYH8NPsdWq+
E9SZrD0rIMYPAePhw+NJBZkAEQEAAYkCPAQYAQgAJhYhBGhFUJwycAAo+jSpAQKA
SlH1cnu8BQJpvUjsAhsMBQkHhM4AAAoJEAKASlH1cnu8AOEP+wXA2I5F2gPy9yt0
gEI4Cy+potlZqHLoZoxlRfDZOocorjIurpw44Nf12ioX3zi2TkEYZGoK+7MMz8Tc
sXn2PWB8aT8ETshS+LEDsrT2i4LpTmCK96HAAqN68N3VxE6mnPt0cOMMcgU1SjgF
6+O/xSiUWWYpUNAXbE4UJArpa9Qui1sAFvWoSNwFcIpUE65Uci/eWJkmn+9Vyksq
8uPG64R5bQQsmjSne0Xxa5pWyF21gvPHvnCjp+Sh7dVMwfqDmOye6GCiw+kYSdmF
r9cOKsED6hOD157QV5jhUQa6nAzMvlCOHNYxRlOCojbSPg5yYQqhku23qd7+9GsA
qE0WnLIeTGJuwFpi6KVK6eZllBMrKBtzU61RGLZ5LUp7tqnltpse6rqytfaAfXr8
ty5r2s7rqktsxSGj0jgwdiJWEad5uDvk4R8vb+9a8qMFMbxsSyfkQo+i7TuN899f
fGdAMHeD+m0P0w3wi9VWEtZzSzFHVXCb2hJxVGBfl1H54clb+1MPdBzX3Kxo0MXR
W/g4/HMXo1uXmzdHPA0o4sAbAlTXYYwuMSeH1IyhCY8LJIsnx0hfFT+B4HX2vtw2
haL5UGNJ9PORA+0l5DBSyRFX1uEwn4bWaXmxGj/dfQLoAnFIJWZq7MVdgRbGweBo
KoAo9nt2pnQWwEcR51eMI52/RRKO
=sAK/
-----END PGP PUBLIC KEY BLOCK-----
```