VERSION DATE: APRIL 14 2023
VERSION #: 002.4

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:

075D 9661 9C1B 5706 1327 F6F6 0CA2 EC09 3956 91E9

And the full public key, also available at https://korelogic.com/395691E9.asc, is

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

mQINBGJPM0MBEACiVEb+PtFBlrbIL9jLjyy5a+lVS+eRwoeAtxLA6/a7ByzWA7Ad
LqNWZjAPJe9W0XTygBJMMvaAyFJ2e3wG/TSlt5XkEZqjvRn/II2ftxJYzntlXOGv
```

c0hK976dDJZBCXJ4hVcSNCTjB9jMKO/cwqvQqOM/XbfJoc9sO2ar4MwcxotaUPQG
stUctGJAb/30oMIFu2jwvH3PFJPBJ/KMZIs3qNg5UJLaUcqxLrktY6p0lkqeRbUV
K+htzfsdw1cg47F/rO1iqXbQ1DJsrbbOF5JXwO6yljpTl/uhporMiT3FSQjrWonA
hvnA9TJNYHV3xZBK7I7xOjrn4d1szXx874D6IO0w2hUR6dGJAMg+tRJdaHC2zJgK
SCPbSU6qGWvu++BjPqhdPYbtyvSwtqEYMZ2SO7Tk4Skudd87VPyo2c/Dlngo4/Th
fjWeeDcWhGh82hk7JgiRUP9I89a11pmcl1gr35FRNi/hcvhYIIY2kqQqzN8Koj+2
zHxeTU4XM0C8ZDZgHcUyTF5MByeUigWY/IdzWvYjS0INNlMctYWC1kXVqvo5CzyO
kNtFHMA35iyTJByw/xHSW4UriEKECn9V70Bzz1QWJ++7UuQF36Y/unbB+JY1mlTj
r+hEHrwTREXakZ3iuzV3cqJOICVeULW6LcURiqpOsA/E5/5aR4ZCrxkuuQARAQAB
tEZLb3JlTG9naWMgRGlzY2xvc3VyZXMgKENvcnJlc3BvbmRlbmNlIEtleSkgPGRp
c2Nsb3N1cmVzQGtvcmVsb2dpYy5jb20+iQJUBBMBCAA+FiEEB12WYZwbVwYTJ/b2
DKLsCTlWkekFAmJPM0MCGwMFCQeEzgAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AA
CgkQDKLsCTlWkelY2w/+NnwI5094j+CaVu/OTMzAruEuo7KHCdQHE3l11zoTp7d+
gomzf6nYSNakBh4ALWoaH/tDAc6iMfbIbhboREbP/gxBObMhIdVL0FvDVcTxFPmz
KgEW/a3dEqZR7e0P9L/TJ4aO8favYgZ4wu23YiRF7b0gHwsuy0jJFU59YpRxzGdD
O5GWPy9sVGvMQvsbr74JlR0cXeBvjKHo/rA4wlBCRxgk6QoUtTNsfICnbShoq7Dc
jVOFvcBfsqmfxagiDDKCuJzvvAL8o+vCYwppWL7tCPVDsgowPM8cbpEwkNyIZPb/
kZ64MkMVcwocvjr4+iHp0lh/jtJUG6Nw+KYms2VGaV38+s+j2nu1M4Rfgttxw1u2
w13nwUeiy4z7GJ2Dbi1FZY+An4dKUHemmYbUmz0dNtv4yjw7ZcdQAmdBhM0PatlI
/3Hbwx9tdZnH/HnvbGwq99m3kC318z/+HjKxMo8KmczgQyLeW+R+ZBwDciRrwGGy
7zT8K+95/00IHbkJGog5FfhuquVZpze22ksv7WgAeBWukONDPB7TqEKpYvsHlDx5
kcYaw/E3bSOkTJAQJjgD+H6tO1CWNQtFSCLbmeumgvmAp1WwpAq6gYjJdyeKFaKC
xltpXjTALqaTlP4pb4QOH53bo1RHK5tH0DUKeCx2ZM8B/dDjjNvYLHH0XoR40rmJ
AjMEEAEIAB0WIQRO3NIgbLzATpWfSB5STS5HWUXP8wUCYlCMGgAKCRBSTS5HWUXP
8+eQEACdQRZjHUTHtt3OApw0tgNh3PwXbNS7IFjbJlX9A4iJQxq2jtz7RszFIP9N
IXzdF2dPF0hx9czMVQI7YUUtgR7Bvz9ZtAMW2SBXlhvQ+0PVtCwffnhnL69HjEyp
dhDqOQH1W2b7wdHKaytsXYSdWsSMGcH0L+fE2AAkIK+0e5B01YXEotRBJHBVQyqv
VucoZw945MaPiDQ5zrc6EicHnM5JyQaxHY5iKp+Yl1gBQgSHsps3JegYyLIDhiio
96il+uzCBCe/mbmEvmdroQxG19vVD0Uxt/GD3wvqLaeNZ7bU7QwDQaJi/0NEAkIx
0I1ruEYtVqV3fzNU62/gQfcSM68ubUpka9Nw7X5MRWVPto8SrMr/gQYaO1aadHBR
6IcJdouoTBOuE4U1gUZP/n6uxZrTXNObwfWAu5/xChqGq7cadk/xQCAbbWB2L9vI
uvPGpuQaurDhXR6RzCcArmZYoTLquMxFfEMlvXwl1C8LJwx4f+ZT6crOpsbfCTh/
0R5FzUEKFV+awZop4d8ul7tX3zf9/vHfX68Nj1u/AEQ2yF93ea/Oniq3+2DHsqgr
Zp/KiF+IxtB1blR+fDP1Sm+SyaAY2yULXT8v9PXOYxVFj5nglCYsPikXIfVaAiiR
RkCM3WTPjlcwq9Un1kBOokc5r6Pwc5OK5es5cWkscXiJxPAAookCMwQQAQgAHRYh
BEbOCayvy1sUy/z7yjteKxYA2vmiBQJi1a9BAAoJEDteKxYA2vmi20IQAIES1DkF
eyUtNlZfPU6/kOHeF4rLnq4QRWyiaI507+nHGbFuQG6ZhCX+HvxvLhDig8GiPITm
PgzA/EiyTnuAqoJ5aGu48u71hVnl+NQ/X7jm1cIqW10MMXTSWfkJ2gKVvyasH0FW
ACiAMBF8VQ7n4YeS7hxH0xJ2n9/efp5XcMkUeiylg9rW3GG05s8eciolKz3TI/fA
4nrzi7CA7uT5PDVSHU/sIF1X84L1lUMV7vCja5hCE/8x7NROoLu6YZcijXZuGz8H
wBTh4UmfdJPbgtsYzUgMpuhzW4KndGfQZC4oxLZzliiUgGkTI4YArbQsa0SHAQMW

0pNXd80NN8h7ZivRRuQToEG0VqIIuZ8emCWlJFJ8OrykkQCO4tklIH/5XznzBW7V
9xhjUkapVNdsbXlCbObsbzIn54WNJOxFO5iJ0nTkqfdNqoi9TUbR+zmHdBdGIY25
gtBsC3wnwfNsJXn2PkVW1O5rQuhgzpD6aS4zIU0NubG5M5/bmxFp6fpYFG6RV0Ry
gw3f77OAEUtOLMS3sRNQQQNYKPfuUknhLYwPnypqDsZ4Anu8Ch6cgjrbHmM/V08S
UN4p0M9WVzgp4eciufnDGmugTA0hB+riQk7/IHVYewX3y2/OYmndFippY/koUex5
7BWIYl/83b/+/jAoV/F0POJ0UvacHXpg607ZuQINBGJPM0MBEACsAO2di6JpoMl5
TnttD/f6fC3fo/C/wZjxYityDhEAxTNiRd4qZ+zJKuuKXoCGZVwLkVAJ8T9dfGEQ
jrMKH4PsHHTgDXU2ieISi7l7nG9s6vgHzpDmSX/9KaffO8MJXv3qEJ4Cubqqm9N7
jpRCnVlGVbBO7Oj/9UiqCavXv1tfsuYyYS/TnishgDTrlyC93ho8hWyHC7r2q7W6
vUghheNr98eeznSnPH+c1jNZfy55YRExtFy49MOusSB68waiwursXGwg89OJNtW3
qIFpC+0OWE8N2QWOUp6W1LjEmib/+CdyOSFdA3Uz5iK6CmpJgn8T6Q9z5og75yJd
nJSwkQ3ywdHJBdD3F1Q4P6Q66Zf5hoFQ1eKwmhlY5FaZp2ntfFFAr6dv6OaxsyDa
frVadKBWshbW4v2GEGh9ea6C3L2GtvJeFszl+V8eJzOMj0HYwi4i4rT9v54Jra1p
KRy+BOPvxex8AF62B1vXIlOtqtBgKOS3NXk0ImSwm28lCNbJzO1pq/tRULHtYsBb
i5pgPX0XiqmhSeRXxBP2kF0vbODJwlu4HLRMvGfkMYsa6VlVsfzIK0PMYPm+Gb0d
hfQKOj8CJ3abHNuVPmloKJlEOiB58sj4WqPXoS8labQLt6wd8mobpk+B1fIkWBYN
/d5WQEZPhsEovu6b+/L10m53sjbKvwARAQABiQI8BBgBCAAmFiEEB12WYZwbVwYT
J/b2DKLsCTlWkekFAmJPM0MCGwwFCQeEzgAACgkQDKLsCTlWkekszg//e9laOppB
BK8APaW8m7iSoc0HUg53lhkJbPue/TE53UGxHuukYQn+WwW49MAace+mEbScy57e
1miK+1JCK+g0mEF/4uJEQIzH+PH/uj5WRYzEg/p/UJ83CzkUQBXw/iiwlNLky4of
lfIU3IbjidPuwxJiu/eM1Xk9KK7eN4Q7H2hLF+mdzrk/C7SLWtgbLZx36LdpvDKn
gK7pF2xHWmttDkaRt75Rultlbm7bfNiwPxTcq5j9rTEZuj3ZpzG9b7WzDU18U9Fy
0RwwGsEgt8HOqkOfGUvW9kHU0P0O7IulVsuskBL1t8LIHxrydbVe3lGYVCPQzg6m
Vb+V5CwpiRXeoKWH3tfgtIdicwL1uPa6rz0z8UGMYQce7JL/vykiVxwdURlRVqzV
OIbUXiHQxvyuM+C5u48X8oE8EN6Z5Xv+wtiC991xZsqvrmJeOiHmGMvwxzzShlnK
BM+26IfgCObgROAjgUyKvJqrPp4hGYbPoAKdQxyTjJHLIxEjl0ZosuWkPLO/jbNx
QLVdnHO0K3AYpBpoyDCR8x/m22kmKl69u6qajhRVtwmamj36jnRzwW79b1xRNmIE
eRbckGiJk4Lrsz8v+5sAPq9v4R5OSNaIZBWVHpBkQmbt2SHB6f4zD9RyVh8tmMEB
ex4V5/1lMwA5uDiCTSdBxL/iDu6DhDYApz8=
=k9tb
-----END PGP PUBLIC KEY BLOCK-----