VERSION DATE: APRIL 23 2018
VERSION #: 002.3

## 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:

4EDC D220 6CBC C04E 959F  481E 524D 2E47 5945 CFF3

And the full public key, also available at https://korelogic.com/5945CFF3.asc, is:

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

mQINBFrOgMUBEADtH+xHS9RWYjg2OoTBZpYl1xMP5/+xuo5I/kcg8pBCw3Q8zacl
KyyWXGm/YiNyNAn/qhHDu27bdsZKZRNlX286PY/CIBL2vRhWIy817WE+yRtTY1QU
UPbL4wvHTklXsvb+BcMFYXPXEmS7yydtmRLPoXx2hq5eHrYKDDxcp+VjXhvjZHpr
1yrltFwbeViwpSD4ozcIc6FYU4ifm0q/BYhiy7+pQ3vt1TKhjXhPqXJwjFx0BW2F
p70kocHGFnGCH+0E1oXRiPOGh3/7ziUUM+4h6vpUMYV74WzRPGlyf3rcjlJuspeO
KyoBaSNGxJ0vWwO7z0keoOWZM9BAgJyrVYweCgJ9+yZqqP9ekjKWRMQVdRtdsYHb
1+Tl0FC/plmRJHcd+H/1o1cyctvnG0HCqB4wLUdZhxEDOkegCnxK08NGr4qzLDHG
O9hOkikWEoMIMRSyvS/l3hfs2gCZIFvTuWrVMhNRfPnWf+v7Y8AZCTGyulRNQAnY
5i1aE5/XmVfjRgndg7TFhnw07LO7Q4y+mJY6NZ50QR1kNaBjOesWj7QsOajPUk0j
AdMAo/4LgCh728CUClal3q/5oBPoMJvhT8ZiFIqVsEy14SsYeSUOTC1Ran/+E4vR
DOI7oF4zFUsbZTCTuFXu7IV3cpE7a52tBFypfszgH12PbNzR1vZIE7pNEQARAQAB
tEZLb3JlTG9naWMgRGlzY2xvc3VyZXMgKENvcnJlc3BvbmRlbmNlIEtleSkgPGRp
c2Nsb3N1cmVzQGtvcmVsb2dpYy5jb20+iQJUBBMBCAA+FiEETtzSIGy8wE6Vn0ge
Uk0uR1lFz/MFAlrOgMUCGwMFCQeEzgAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AA
CgkQUk0uR1lFz/N5hRAA1JhCMTSpkFYN4h9MWy+BIVRb/MelTe0VPafbRcAoWo7C
B1Hj5hmiRF8rEVCLP6RIcSpNkBpgwxG1ZBRTJ3gBDzL2b41JiVFGV9kZ8h42xFHr
vRhn+fbzL9nNUw9wAYQhb28k8BA+RoBQ3o75wVO/vefW4mA8q3p+RpJ2WpafrwrO
DgmWaGBkPrsOac+3mkb5as47T4IPXyIK3f0fXBBJrSjq95DFb7Fz4HlJmP9NU1Fj
taj7Beokf8N4CiTpv/VWquULI1uNljrjqy4wa1z6/nCy+QuWEZTMFyc7KKbzYTXu
5c59lkgHCM+q/sAhPSsMYpuIDl6GI3Ea9pfoWWb3O3PMOQ4LKsrBsdnZpYfdMeim
q751zTk2BCjZrW5m2zUz9CzrEe+DE/Toqrw5v7KG1c/r4+8Ur64PG8MvHEnwGRpP
ySNwGGpgeMNdupIZpP+UxAj06CAzeDdf0RAEaos1ALxTy+lfGdMib47Ppf4FJIDb
oIL6Ay5CiDgSu+dxP7SnYZJzKCC7P0iNftDUoZf15ESW0VokbilGOuuZHvn3yGGQ
NRDtET6hUhbq5iXldo3ZJYrowXyRC/KOEl6uDBGrYhCiu1skezoMFn/MQ0r21g5G
qRrSIEIVTUeyoqSBPyaUxbYdYrXFRwQ/d6Z7UHFY9UxVAEy45yi97VHe2CHxDr+J
ATMEEAEIAB0WIQT5xKu2nmNAkS2trvRNZZosDhmJDAUCWs6CRwAKCRBNZZosDhmJ
DMNgB/9j7WepBj7jlBbehYXtZC7OKHKuHW8VTaJbhpsSbHvyCTAWCFkPWmdekjNd
IbM/hlUG2Bv7Q1E8J1n6Dh2gNCmHtlHP0+fU9csPYaFym2bkeDROeu4LC9a/HPoS
JMxb8NSPy6FsAcxK6y+Mp8eqe/S+BwrhI6pTm1xKZxXLQ+JbAV3bKUEoEoJ1VwZE
DaCHYDSQcTPFxiFVDyx2kzeJlrmhFuYVbeTqf4K4yrXFn3dYy4Sxgxg4/Vo7wCHU
MFeNYIKW8ohKhBHS9q4/iF+SedHLrjnVkoHU2YCXXpcxA9iT7EcBMCy3RM5W8Nu/
QNt3QHkjaIIexI46yeP3kSwHxVdwiQEzBBABCAAdFiEE3gGHYacUYYYn1xm8gBtc
0DnJi2sFAlrOgnwACgkQgBtc0DnJi2tqeggArePI4PPtIYsBBAKHFx+RTF+m4x8j
EdJ9csgF/8kXSR7bpknYHmG4eGREFmX72qlushhAnRykbr3FzxwCcMWKklYIWYFV
KttRB4WfDDFAUDT81j67C/vVWVVg4dB+WX1skl4ZpVf1AAX8LXXw4fgI7amo+Km1
Ft92/HjuiZT7HmjnHD9n6cD4sZ6Jg2TGHTlNj9lFciFWbamavmuhEiWl3r/0VNHO
32DHlTsg2vwfbSDJENv7e+rGXhPydNvsNsvO67RawX9/wkwin8GUbzI+yekSonQm
1zlyx1ZRoOJGC1sTclhgm7GerVUnAmR5F3aNK8nLOPr2Y2+cEfwqDm0cU4kBMwQQ
AQgAHRYhBF9t3Mj/U4CT7DkSewkef3zomOhsBQJazoWmAAoJEAkef3zomOhs4EcI

ALA+5CMxHiWsEgfzz2BqCYOrEjT9PMQk77l6le7jsY35lN29HBxZIRtFqjOSoFt3
Az3PgYcNSlQi2KKZYZCCQ0VpghwGsJnZzoc0RppJVEHUaTa8qNMNme+c+OIiJRdl
IOQcjNMalcFOj/zRRdRBRnly61cgC/drvJvgzl1h+4AkJmlJo3uojW1ighNscDz5
WrTSkCq6Wmbh4rlMawgjQNBTKFAWgPVZrq3ue7/V2KMxxhCXt+W39C4KY9b+0Pmc
vBqYoVcLzRAa6CBzP61E3hQiO6E/01+gNPsRV10GyhUjlyg2XavArcJ3Pv/6leAA
KeAXD+2J136ZVT3vjKreCuyJAhwEEAECAAYFAlrOiZUACgkQ5ky8nUKogxHv7Q/+
PzT/LtqLUK+gy9EQxvZAUMroh63eKg/bQimSZC0hV1ZAhumGQuFeHH6ur099jzjm
B2esXGfFyA3q+cD8fudCz4X7LLOs1zSA+ifeO8tIDdebSXhwXm5llFBHnCRoPCPu
DahwdKJFTb5AfI2TKxu+pgBbUJd8Ejdbu7R7C1K7XbjvHNscotqMrqyUle9Hf0qQ
M0G/tOTr+GC16/iDnyDMbZwzOl7XBHqclAH6BSiOU7Yu8xMcbbfWhPasjh4TmQMy
nVimNMhptdxNg/oDfoaNV/2EawXB8OUKbBwWO7YjazPvgE6HaGrBc0K4ZzHyHj5r
TrY44ju5pxm2TFfvy5UM0EXU9Xq3UuVUq9lX3IUlsygk1eY9z6lUgJYHVTORXYuD
uyUGmQzXQjL0pGJdCdWnKj9wAEJ1GgKXG38YKEaNNWi1ak1bEvT6Q7sVxzar3Wvq
UXrcQpHPIu/VuebJ3ErIqHs1jgXqzskmBnoWADQm32VMxc+tpWHg2NK5SFY5NTeD
8fCGenPK19nKb5sDTJV8jmxYBq4WpnLquo+PCku2ZuJG9aZiId1XWw1IBxelY03f
BpeyY92bLS5eT2GFs8NuBwpt2YdF2TUu/gUjH0lsPmXvVXLMrHwVklUgAZPgNXrv
OKQiZdALzLdmX9OLId/7v2uuSs0G/ovFNetY6qUwklaJAhwEEAECAAYFAlrPPo4A
CgkQymRYWaMGnBjosA//UvD+omlBmZIDsIzlaBoP7um/BpYbEIe18iVbLeS0bC7l
GgiEEY/l1TMF3DnvkRSlA2SgUDTt24il65/HP/9cAldpp5tO2R6Ee5S1e1FQJ2Up
YNLbHQEJJVb9yrLzPK5Cf5f/uVwZMLdretXqWKwc+SOvetGG6MOA3J9xfbSj56R7
gZ0dEWvjWD3FXAM3sHHqo6KdFgRcwIIAQakld1Bh3S2cJt3Q/gN7LBi6XVD45S/H
q6vT7tlg1JLgZRYYlRVQp3hD4RafI8ELQzMostq16DEX8AGJGZxQ1q5vPeWq6Hrd
5cLjJt755s1SnjFiMhSXl161DSsDKWPXjrNyd4cTmdAndlCkYPMSKn40TRyciPhn
Tg6o6qxRZt+fIziUsPln35mz98wdUOzWlWM/EFy8ibbU0k/TRZ0DaiL7xgQwyGnJ
FWFSEWMqcgVBAqGG5nF61n/gWxxhRKoj5V8B+1/lS53D4mIcOy5xCHJwOawE78Yg
XTetvEZb8rMemmj7i6l+7wuHSRQnUY26xsry9Wo+mIERVXMcLTdA0IfC4yD55lwB
fOHbKCX27Dq08W2RVZ3ZD+9DSd22A9FX3gTpWD+QWVvkN07+ERVj6hwaS0Nt4Y8u
7N5Pux0bwQwMB3e2jXur/EN1j0AL/PC+ZHO5kCtLRB74gd0/g81sQUVfn+0bNAqJ
ASIEEgEKAAwFAlreOQMFgwPFCgAACgkQWQCTntDEK09kPQf7B/1kcsjR2XccjhnC
2GWAfV8lRTXt/trzKkO2h7dxNDPqL6mt/OWzZWMyaGNTMGdQMXSUw23mjRsfNU3y
H8eQv3rNytmcBvTn6uZQAV7lkYQsgpCy5nAYvqgMT+EDLbJhhe6einDjA0d+NWLg
QSAxPwNO0V8Mo9bqF6bBQ5JEPPoajR7N/VfNCtB59YYAT8NUZ7siP7XCq/nj3+7d
tX88RXMxIRJc8i16GRz1XCgXzPNbY1sZG3zz/8v6AIW7iHRU/e5bYj+NzlB1BMXp
V9Npb2vYh7GOamnjMBAHGJA1otqrBPXDiytYEAeIuWke0lf8gVGWpEUWvjnBzCZx
sK0YcrkCDQRazoDFARAAAxQNVrVEkixHpmx97srxGbPcqIjWpeYO3GsilTBw8Ed6c
rnsRGwTh5xa0BS62HljepNGM2gtYX0OdNDENg2JxF9C1wnP0j+k6OGO2Y2GUGvOd
N6M1KcgOVJ5m5FqvTOqr/MCHjMynPZJ+hnxSF3E6rbvceGSHlco9i2GgaTfKzIVh
J+i6Ytw4j7qgurPl7UrUMeyXw/dUYpiv9tqtirnzj3sqeagT9Sp6+Vu0MJVR1mST
6WCQXFx2UU8scp1dlTXou4rrheKulB7a8VcZKNExjLQk8Po+nZvwLEO+5nk56jjE
LOJ3qXNKpdmH8qpi1XETaGd6BUsnB6E6hf1rqwGNzhYw8ghVSSDxd+pYjHffuBg1

YlL//EAhSSg8BlE++uuRci8eHRmv772b+8fg1rwwi4OZcVOUGyAAs+z+iUSwM21g
BMMGpb818EM0Enl1kfB/LO0I1OVc0fZxDc1EVHk02GrCQWgqeTwROrjpBF8ltDeY
I/BlZ4K/mk4gZOKsFoLrritZtGK24q5kQavQq32HrFMFrXabMZgMULCQ1KgDTJDH
Ce0TwL7/bgFNlfTMZPKe332KCntWZEtTbwMyQt6AWqk7R1945OvShhi3Gk/jptm5
WMMOUVUQUZhCwf59bNzgSk2FAre0SLmaEAIgo11FzUe+lIwg4NxsS/w06+oUERMA
EQEAAYkCPAQYAQgAJhYhBE7c0iBsvMBOlZ9IHlJNLkdZRc/zBQJazoDFAhsMBQkH
hM4AAAoJEFJNLkdZRc/zKu0P/3lVuq6CSRJDQTjf/6TgdUwZycQZs6uCjv1j4l+1
5U2QZUlqnn6sO1BlZ+iSvKVqb+SZMs5r9cB3fKeNAoaHqtMOyK1SHYSZRxvq0tFW
U8L+EZNMLHJHrMYUnH09Ix2CeYqJmwGytkUFVq+pDwwj+smfQuZIlxUtjEwy7K/4
pvk9jMd6ehKrgVk2De/8Ggcxakr97qWmQIbeCXgLusgn9wnmKjdxgFm6PJzHI+Fp
3Uc8maGT5BepKcixXnyPOJwM0Udkh8AWUaMt4E9vuf5FUShSAZRJlHvrTrP76qD8
fZbUxoMYits6QfUTS1KLMtiLRANI7bTMve25Y7jWcts/pX7Pkm8a4fQgMvDErcp/
cDbGuRcjqDzs+nKDn6hNqP+CHzT/y/M3+iOXK3dLuzO0u3Ktxk/7BCQcrNa6Ke4y
vEFikH75Z+s51u5AsmqEIoF/ru6k54fthN2Z+DdoyqhAxh510SsK/sH1icKdpC8S
vn0VHGKc82dT+ehYh79w7WLuN8yhON1y6JLhzwgixHg46qi7HVFSpcZewLltVRqK
4I7LXy6UspSXU3f89vB6N841X4Aji+VFxmDYX86BZOmwwECvrUEjVbFQrSBpqavm
x1/OAsEbl824UD9gjU/uvfTlO1q4chkWl5trdPKEGxPKzFfKIUiN1e4LF5t8pkp5
2ySO
=JxEq
-----END PGP PUBLIC KEY BLOCK-----