KoreLogic SECURITY

VERSION DATE: NOVEMBER 4 2015
VERSION #: 002.2

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

KoreLogic SECURITY

VERSION DATE: NOVEMBER 4 2015
VERSION #: 002.2

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:

F9C4 ABB6 9E63 4091 2DAD AEF4 4D65 9A2C 0E19 890C

And the full public key, also available at https://www.korelogic.com/0E19890C.asc, is:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQENBFNMHP4BCACiMgoN46WUOcblv9KY3zd8+tBihJz32mjPUUjyf/2gmDSIfbry
1GGw+UdFpuswMz5WaPQMT7p+s91COUXxdpgmFntG0G1wlbIk64AP0e/kHkQHSOk4
Yw7gWyJwRx4KliDZHER+yAfdcG+Ds9X6cBVs+bNDLxHmhgeVoIweoFVhCRzrGglJ
3unVsWQpA7uh9dHNgTmJ4Y8EUzsYtNoxTtkmD/uwyuX/Zyr+z6g8RgyTs5/0Zqu7
NzlzuVc9RLWbzKmThYMK7+ml2L8pVvSQcKLZxWM5/2FZqXSA940n9B5fKJTPPHOh
nHtCruBnkbrzP50CVD9KEO5yWwVFYcjwvIHbABEBAAG0RktvcmVMb2dpYyBEaXNj
bG9zdXJlcyAoQ29ycmVzcG9uZGVuY2UgS2V5KSA8ZGlzY2xvc3VyZXNAa29yZWxv
Z2ljLmNvbT6JAT8EEwECACkFAlNMHP4CGyMFCQeHWgIICwkIBwoEAwIEFQIIAwUW
AgMBAAIeAQIXgAAKCRBNZZosDhmJDEaZB/0Vy32ZKwrNArA8aL7GKgORhQW3NVPu
PhZlCnkMhkVDA0Wc13B7mg0bZXR2cc3Jrr4Hbta9AULL4YBrc5Ku/iWMJLcqqdHk
fr0dhhJ8vt0NMvs5/y+YwqO0cszOUYMBuxEh5I1zZ5bXLBHL7jyX5q9JEyCMpNV0
jDwoo/mGWGbOw6FoGeShUTHBY2xp+zY8pzoy28MgjjHqSMFboQ2s7OtokwZzKYFi
aJarp0XeqLnqxAh4NFOp7PNpdI3xAt9k/F1PMQtosQqQ6NBhOkycRT47Eqa7bRnH
iQ7laHQPMh3IfBiAXEMDW5bPQOFXtkZTmV9509dQlRBLTgw4d0y73iNIiQEcBBAB
AgAGBQJTTCB6AAoJEMJo+wIVjIfD5GUIAI69JtdQN24ru9J3no79pvBrN7wbBngk
5lCq/IXis1jwaYPosKmKv+1S6idGlhOsyq/2h3NXOjRxDMj7NFNz4xlKZvNqI2+v
Pkg18haTM2FdFjMcv8Z81EmhFbcv1dhnu7meKvchxpXFf7FUhYU7hvqxtOP+mH9S
zjMr/LcOaVcWvMic6FTbNtA9lZ25+oqlgzjOcop9loolоWymzzKjJ4phj2rQpF6R
B5EM/PRVTeKmBYqydO5MsxAHT/1oZnxhV9Bq9VM+GIbIcAh/RsazZ0LRgxuPKnYM
Yw340/qc9AYaC5OIdGfp8K5QKzPBpNApk67pT0np5CzLDpB17ha1qv2JARwEEAEC
AAYFAlNMNCAACgkQmqG588A6u7rm/wf/bnsflueEtmT0EIXFxFntYjZjEXWSOd4p
VzLNduUH0cQW/UBP/J9+HHMUgecBKUduDGAYclPukYcsRKMpxBH0xwAzkPQ5ztEg
```

9fZkqsi2PgItfpjtrmpP9JAyme8ILJOa/3mhlD/JPDKEYV6/2QIjHQHtHtz/Inf7
DFYjjm/WsGhtYlmLjBcwrsoVo8rJv6QVAft4g7J98FaMRHN2SvtgsQQZNUPCoeca
HcTMGuvjGyany1Q0XFFOQURhj8t9Z7V4XxnGyw1XQVfWXzgsCMH7EfPB0oQALp9p
Gz3v7Ok6MO1lizL2oEFGqrHACYxzhSJcea+wcyAexUmcKvhncRRRdokBHAQQAQgA
BgUCU0xJpwAKCRAtVzLhaGtts9z5B/9R+/F5AWhVIDIM6fXh6jQtfDYyinVvV/uD
p/RJ+p+GzBaBJcmyO1SH6b1p08g1ILFXvoE7QVJY6movMqJkyz5qBMzfwIhNbtvp
G7g/1Vqjt4CtsGJ3fbYgkH0SWvRn9B2UWBGZDDZC9YdKETTGEsuHwXBl5sVQyl53
a3S3RNDeJSE3zkZQ51p+N2SrDdKmyrxvDddMkV59+wMQ9GLcje5Fu48L8KO1Rykq
oRiuMsdn0tKHtSigf8lDu2VgIaqk0nDk3KCBp9xUMMKHU261ylaryXmS1K8wrCKh
vF8W9e3iMHHW83RBDHOk/ARcFsVxnvgXE80rsUzQOZh/i6RUgfWWiQEcBBABAgAG
BQJTTIrxAAoJEKV1FD8Vg5MO78gIAK46RghxWoC/+sjF8N5CLO9SqD44RvMio3TP
b/rMwm0mq36aUYSjpzIK1I1x0Nn1OWnFiotTVt/lxhSIjfMp3rC1Pq9bWG6vWDCv
c8CqmPIp3detuBiggXwrt6EIoVWxWeYMrFzSy38e4qKmtdrowhRC/e5Fa6Mc3Lzu
PTKJznBsA0n4g33R/ut2jFZwwYjWYCxxdf6EgBj7u+jjxP4n2QHgfoFxcQ//Hrlu
s4EIWGwbkmKABQ6dAWynhC28BQTK5naJisFzhIZoFy2003MGVLLDtvF3Pb6LGP3k
wT3IPl9tRjGIXnm+vI4Igsgm2stSOJsOL4AYVLQnK8dwewgxbEeJARwEEAECAAYF
AlNNCGEACgkQoQY0R1wpjbsxZQf/dGimFBY1Cdb4H+sC/harFWHoVPzypS4J7Y9m
PA06WCsUEiF3wXdoqcLVs45oGjHbubJY4Wch9oAYuaUe9Wkebf+OtWEz3d2ln6DZ
Pvl9hNMqmxdtg2Gs5F6Jn9/ZHumt0TQ3AMFldbYlyuukId2gSo/EJN303LMoqMRL
sHb8IYQl/n4uXRp3obZlr6TNaRZ7FZTR1qJAsWBSPRcxDIBP+z007DR9cqg+AwF7
jKYe8pJavxw/lLQ5xWKwzvLIlyY3rJmoGGhnXt09XN0ZZLLDr3Z3E7ib6H08dq2A
H2A3q/JHVv+aiQx774ymQ1KY/gz+ZN73iZaobKjx2UFpUa+rqYkBHAQQAQIABgUC
U0xJtAAKCRCpM26ZTizvdWXDCACLuns4M+biuimQMRltY4Og/VUX3skSqEkQL1nE
gOE2J3hPedKvcnh5vT/JWFjCieKn94QSeWpXzHz0rEcyC8SX3IrNbxyHfmXcsUAY
V2awZJbLXwoc3tpz6LHa5AE7pxlHdRjtR4O33wP+p34sRJDwmhL37Zc03rN0MumM
7iqBbwtighPdhrAe0L4oYQ3iffU9Zd7/OW9qnAWLKDcvAeSxTmdY7XPbhhfrEQ/6
CMnXvncFWWWQbn51wPJNykTjxSLLhR7Is2ixWk+2E2PSDPNboiUTouIAUkQRJIeJ
gOp6yMijHKi8dt/hMH5p9eZBMNyr6pPRu/RvF1lYFF/eXWS1iQEcBBABAgAGBQJT
TTZGAAoJEDRq2MAeRuDavU0H/3n8lxWvMVuB+KaB4mwWulpWxmVQKmXCQ6ZqfaKx
5iHEF2ilKaCM1npmTPyfJhK79MDxKtfzQLZRDf8ONKmdV6tUmmRfnaMGmqlkNatb
zwzRgNheUVvI5SHYXrzDmOLwFYEXvZUSAgHN5WmxI3b8JmapBuvP7EJmgPcKoqD0
hwIZRP9lF7obNKGuegUeTDq0hdy9Upv/DLX86rYZ6Lr/bZEbRc/0lgDxOOth+Goc
jZNSlEO26sr9m66JvFGCSB0SciJPTgT8/FzyTJ5lcOwmx164l7YHAJkJFJJltegg
mZ9jQEV3Okyj6UJiYcNFQyOXWGdSzHIntulHypW9WGy0sReJAhwEEAECAAYFAlNN
UEcACgkQwN54gtlChySCvBAAn8Am1HzZiIh4DLTBCF6y53K2G80J8qWKehT0tPV9
34U7F8vLKeYMs5tT7166lDE65ElTshP0f8vAPAoI3e7Ph5LkP18Yji15CE0MhkDG
AJm5WPxw7ofbVm1QB/lmdofUXZb3Pq2RpAqswV0Bwd7kuXxMaCkti+ns6P6rrRid
s3TPGrviGBSPBpaY5vAK1PHFZjgyz5k5FAVaQnUPPGtMoH2Zgfu0NuDmdnuUtNDY
LdOF748b/3lurMrp2KYLal3Bwf30NJ2WXc9UzXKdrKAoFn9qzddngFKDSDW5Nu3n
tRsy+S0hDmnXIWWQK56QHN05BsPkMbwtI3u2b38UHywKwCRwbswOXYsPyzSC198a
BdegtTFH7sq9FFN4zfFdf1vHThA8nPXmBq8OaGvNz6EZMKzElKc39rOzCSuIRoIE

Zy/sLQn4dQF5tz7oZ+3yC+y7aQl2VoWThxNodugQ5WbQg4UDEsQ7xclq6oeW4e9j
qAFpXfP05ywvsRcYHKV/JqP1KL9oe8FDfSvBX+VQSWECBDkujU+r01ayZfYT9c5l
CqyFH8tC3HAftP/yjd5e76jCVE82E3Mj9l9XyodMSDi7wjCiJGkb64T0qhrtmGCJ
Gf7fKhyRSfd4abYU08HKlXgLhfWSXtTQWXyVFEfiq9TwGsyKKPopxNSyIT0Al7Uq
zR6JARwEEwECAAYFAlNNZKUACgkQZd1HfDns2NHbTgf/RZ/dvkCH8nqw8Ejh0zWR
1b5oSHHYTJ3BUFo7nVh5Q7/UmjyMGLQpsoSkJ2MDdmpFlDy6ldwuo6Ulh6m8YMB+
OIN3M3s7bst9g/TDnTZ1lgX3LRZYnp08HwfNLzDFTyyQY6nzP+TqqEyB1M9VXCjq
zkC99EY8Yk+LN4XjGca1lGynRRzMn5F6UuPxMD+nOQoWA1zAp5AikYcDsjtY/dAp
4tlfwLgWKOA/671XIzRGkDzycge1qZibmz1RuTDZA+YpI2u5k1w+dDNddymUV82I
30LGUFzynoDwvgVcMHD3D8iaTu3rnDf/MypKJMQH3l3r4HqUJVfQBw7SMLHOSq8p
/YkBHAQQAQoABgUCU02BugAKCRBZAJOe0MQrT5QsB/9hTmeum5IwHlBVLw4qDIkG
YWpHgz7ogw0dSvAVFCgTakIdR7Z12QWS7Y3gMVwowtVIOoor1/nockWI+2XXS7Zf
7G89W+SiTeQhceCu8QsrrHCrMT4q7OL+LlWJDfnICzu9vURVa7v7Q/ruzegjUsye
pt4unduAbebrCyLZ4Lwi3Uxs68hf859XMiPaeAXKMg3lvw7MCLS4bWhMIuE1lYYk
vT7onWaq8bvUi757uLz0gESuDJ+MMHLtfvquQaAk3GeIJekXJmnVbyN+6+lgRvaa
irFngeVg37QceAEgV2NPgeI8gbuXS9herWTCHO6+o5gIeI8XbPoTuuAAzOrGI0h4
uQINBFNMHP4QCADZW53cZ0Xet2h4WyxZmVyo/WAA5aDix5zzbu4fD1dHSShW9DTC
cq3B+6D4nCnFEaRQqWiCKL5jpWxhoXJknrfXYl3HVjqXSko93db5WoPDkzkPXaJr
QyWRndy9QLEwXUi/kFCBygAFMStXECUFcvCnVSF8mcipOnLVeLlQ6mrWApuPCQen
5UtpyADhBZtwMQogeVZw113XpAejsTh2HiHO/8NvCXAtT10/HhbPG0d3uJajYc/0
RLLk+Wz0qDVGhzg27SxnLKEjDYgSXwN9Jp7fy3HProE0vW7pSv1sn4UqgQqDKqKF
heHGtDP6EiU9AGXOhhZ1o6J8NF2R7yNrW9nHAAMFCACtx3/8h9rzGUROg1K9GrHq
A4vFxW288M7Ptjw1ElsmOnsim/Pf6lir512GVoHTuQZecCnhlAjByIrhq5QojECv
5bO/FjPt1H30zUwNTzSfFDmtHDBR1zEqBUXXx621pJXNyqCxBjVbvHAegYEwI8/z
fDv73L6MtPDsCXocuWYWIzrWgRSJlrh49IlCVe4zi0YoSinxKrX7opfim9SRCMyg
eQYDENWV6gPOKb1A310MQ9Dowt13Qz7y4+oh53XaQ+1yWwHO/84vUbb0Egc57LQY
wv9LBHQ4+Lc5P1zos9jlXuK0RHHvFAl92346TfoIMzrGTBc4ZDfevkidJHQ06KmM
iQElBBgBAgAPBQJTTBz+AhsMBQkHh1oCAAoJEE1lmiwOGYkMKsYH+gKE3kMNO/Lw
4UxNr2UZjMK5GEnxvBr2AkksMys2WatKhRsXiM/eW5bUfstVSIEnZaqRalMxg5Dn
Dx0QnNqHxFTaO8+RCG7n396vW8NCb40Cwm02WmQ0mG2NOA6N9VtIW/4asvg3rXCB
mxVM70BTkZJdQ5hRsQFBKdl9HUSDK+pJNz2+sBn+IuLbHLg6WpEeOSErba7LG8eP
KBixUnImPBngRdmAIWpaT8mbGlw1VO+GheNlBXf65wyIs1Z2UuCP7J0S1FsJmcAs
s6ESEP2kde/b+yGAGc/5NCkWF2SsR6uErsltFO34dTYlA3mhl6tQl55eUM3L5EFy
HO3RLTN0o0E=
=jMQM
-----END PGP PUBLIC KEY BLOCK-----