RFC 2350 Description of EnBW's Cyber Emergency Response Team

EnBW-CERT

0 Information about the Document

0.1 Date of Approval and Publication

This initial version of this document was approved and published on 2022-08-01 by the Information Security Manager of FE IT.

0.2 Notification Distribution List

None.

0.3 Availability for this Document

The current version of this document can be found on the official EnBW-CERT website:

https://www.enbw.com/cert

Please make sure you have the latest version.

0.4 Authenticity of this Document

This document was signed by EnBW-CERT using S/Mime. The fingerprint of the key can be found on the EnBW-CERT website (see Section 0.3) and in this document (see Section 1.8).

Document History

Version	Date of validity	Author	Amendments made
1.0	2022-08-01	Ulrich Stadie	First edition of
1.1	2022-09-13	Ulrich Stadie	Left adjustment
1.2	2023-01-01	Ulrich Stadie	Adaptation/update due to the merger of the two CERTs: EnBW-IT-CERT and EnBW-CERT. EnBW-CERT is the new name.
1.3	2023-10-02	Ulrich Stadie	Update PGP key and S/MIME certificate
1.4	2024-01-01	Ulrich Stadie	Update list of team members

EnBW CERT
EnBW-CERT
2024.03.22
11:25:33
+01'00'

1 Contact Information

1.1 Names

EnBW-CERT: Cyber Emergency Response Team of EnBW

1.2 Postal Address:

Energie Baden-Württemberg AG (EnBW)
FE IT
EnBW-CERT
Durlacher Allee 93
76131 Karlsruhe
Germany

1.3 Time Zone

CET/CEST,
Central European Time/Central European Summer Time,
UTC+0100/UTC+0200

1.4 Phone Numbers

Urgent reports of IT security incidents can be reported to EnBW-CERT via the EnBW-CERT telephone number +49,721 63 12130.

EnBW members can reach the EnBW-CERT using the telephone number known within EnBW or via IT Support or outside of business hours via the Service Cockpit.

Telephone contact options have also been exchanged with established communication partners, via which the EnBW-CERT can be reached directly.

1.5 Facsimile Number

None.

1.6 Other Telecommunication Options

None.

1.7 Electronic Mail Address

The EnBW-CERT e-mail address is CERT@enbw.com.

For reports from external parties to the EnBW-CERT, email is primarily used as the input channel, provided that no telephone contact data has been exchanged yet.
In urgent cases, [important] can be included in the subject line to indicate the urgency of an e-mail. For encrypted communication, the EnBW-CERT provides its PGP key and its S/Mime certificate (see 1.8).

1.8 Public Keys and other Encryption Information

1.8.1 S/Mime Certificate

The public key of the EnBW-CERT S/Mime certificate has the following fingerprint:
AAB1 9079 E7F9 6EDA 8B55 23EE DD99 21A5 4E50 6DD2

The public key and its signature are available on the EnBW-CERT website:
https://www.enbw.com/cert

1.8.2 PGP Key

The EnBW-CERT PGP key has the following identification data:
KeyID: **0xC5060B5003FAAE32**
Fingerprint: **C181 39D7 3410 A204 4800,270E C506 0B50 03FA AE32**

The public key is as follows:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGSVX4UBEACjFZ9n5MMimbaMN2iE78nA2jfD65oRm/aYfJQ1yPo4tfqj0ysc
vdPiMXkVSX9cMFr4h494sHbFR43rLjxNQlb1ZTHcIMP33GM++HCh3/P+HzeNd4Fc
lrMhoIfPQYrSPM9jVHyDFnlhycueVbULF0+hajW+/cZpoWQrPm7z7Z81wJE89q+j
jRsjS2iOTCTJGL2LzILQb1jXikypW/+xdjW98rZwhLCJRHS1MMSDIRQRLqfDQApi
/KSb3KkUVpL0T53Gz11x8pyqdHYvDcqmRtIUZcm8Y4gPs+h/c3Mpy5ONiyxPzawz
2shAOlenvnxCLF4iKtZqzH4m/5qPWxwlKMkjFWPwNNU7Yp6tUuE3Igt9fhQb4heF
bxoR1WJUZtTNXxV4DGe+iVzWGCxXfP+ll2VS/6G38fj3i2kXM4xHhnCaHZcZOCM2
/RHkT/mNQerGkGNFaoSvjURdy4sr+f1IPjFCxBDZevr7j/ZOITJmriZKBYC6cTyT
wyu01P3phVq9HsJBq2nZdniLYzK0wsJe2+4V005Jc9huwKZpBHImDejoz8oIZiI0
zVmI9ikd5DtqxXryH8Qo3au64tIV6CNIchl2dVDATqSbTZd1h/DzqP4ZEu0oTzab
E4FR1i0FZSqhRaAJRo6p4g+BoUbgSdiPW+S2D9kHKmDrDff3q4wsamBkswARAQAB
tBlFbkJXLUNFUlQgPGNlcnRAZW5idy5jb20+iQJXBBMBCABBFiEEwYE51zQQogRI
ACcOxQYLUAP6rjIFAmUWurECGwMFCQWk+ZsFCwkIBwICIgIGFQoJCAsCBBYCAwEC
HgcCF4AACgkQxQYLUAP6rjL3yg//YE57BayOpLEqKqgN3PQML/R9GQnfCMHwGH+i
7shc/svaQQglZutgOPM4qShxLzK8TGpJ4cdKhq3HCgpSehk5E6szaRBI8CRVGFe8
mVp9F/61j1xtC0kCoYQ1/y4/KHV8vBZWITPBpmxItamv/AHodBJ5xz3prGoMwnRM
pNi9zpKM97WWNIA76aOOY/1j+/CrZSAxtbbXrHdXkoOEFTzPPFxqgTfoo5L6JxP6
3Y7Pg2c8Xv3+jqLA0xzgwnK+9oxhMs6X3hjEOt5+QfzHWiOdoqGx7kd23wTC4rQ/
Y0SjmIupeGsM1ZUJpMdiwIF0SPawIvmU6gyWZAiuFRbxZfMOd7dkS25TDEbhmpsd
j2lrsILrLOMTmvUkkzlCInXhvidQh+fdCfWEk8xDjbA5BRRBYctF5BMR2NG4xVtc
ipLezgBjsuUJecQLu24KlNkEtJ2nmiFM01qpe8cCyrJ43E8PUMLKMauyUjmrrOCR
nLoGCJjLFYaT2Ir81RPRHx9Z/meZ8AfN9AZwg4pOTzP3ZMLG5yfYXv8OOzm3/KEM
vFdRoEkPbu9F4vgUE3LEH1Ipiz4poV8G3SFqVTBZCkzxGwmYZmW2JXP2RrS1IgCB
Gkx29Tn7m5nX2CwVGmVhtSu30GAyymS5nqulpSpppW9/vE3R8G91TNrirhsqbrVV
j2lh9L+JAjMEEAEIAB0WIQSh9B1QVfbD8skDJksE7dRoYt0wNwUCZRa7HAAKCRAE
7dRoYt0wN/vGEACLYPhZPR6m0rhOqrZjcBOLvWMx813q1galYmWaMRFrbK6kMXfz
sxx13e3okmjfwIMVg+DR1GZriP3C/J8GFUuDp676U1bEt4L/kJVU/CY3KqCFPUk1
Dzhjy1FmSccDDL4aEONhjsUlu7kkZ4GtW2Lv9AQVsFPEKKP4y8BiToR7t89OiMlq
nNlny9WIh3vqmfjmY7sz677/Kn8sX3fYsiZcum3Re9rB+ScKCQAsdOCqrV4zbdrS
Z7RNqBIPDm9sTUUGKFwbG/8SzYQk/c5R3A2V6JOAga3hycpXEpzY6laE2sqkWxIP
T1G6g0xZbGxZZjfYbm+NWbji7/5t0dZVl+p2JKF/JnKEYCrIiKIrG6WzNYIGcCX7
IjXCoxACA62vgtZJVz8lJ9BeU7/P2lVD/qlJCII0XDUKG4HOEKNKMPnzJyzGgeAj
KIVqxmgimpQv8fPTHn9IJUBRVGwbM4oVEEX738lzo+UoH8MHgY4c8dtxpwV4UXvx
3TutM7jNYxZYfiO6v/mdVFzdAa5TvTKEOSeJtnp67DToJK7lM7EjZ1ockzF2WMCs
7k408+Ildp+sWwNG1N7lu/09++1irs6GB+sf9w5Wrr7sbZPMlhubBpn9nNYImRP/
FwS9pSvFrBz2IsGpZhwinHjmro/j/+TKJFI5dGkiXLmxOtcSSudipP3OCokCMwQQ
AQgAHRYhBKH0HVBV9sPyyQMmSwTt1Ghi3TA3BQJlFrthAAoJEATt1Ghi3TA3AEUP
/0Ynqz0ZWIEZxx8TGrtu9QI+wLSDSM7a2z4Q8uGgZrTh+PqaQ8WZ+/lHsxvNRHlg
hh+ADMPBHPeuxkYyP/uGzfaq8qxQK0U2anqubjAS+8a/XOgyqUodZJHH2TqqfHyx
ya+H1JIatNoJ2rwoMQ8hbSeVF+uN0GwzsIAQGmmcITBsxq6RmEgbNC4xWyoNZ32O
TmoUBcz2upAeCmDmqTIVVhS3hS/LkwWA2BmLJdM47arVZ58LN3P/Pxy11yleJAlx
s5Dw2v24tkVK6qjfF06NPwAJ+epRhzcPoLX8RA9wgB1jsF8Wd27PlgozEocmuOVc
oQCGuNt5YYhQTXyJZragoGrcpg7QloFOpEuXsUdtC8h1PYi3IkIyN3UQHBZVxsTZ
6UkRS9hYu7HpX1H1LvROdbUIFNvwkP43x+ZztoJOp3OhXrdxk82WdkU6BOqLBNJ5
```

Uh2pgjrSNYe2bT9eDifj8Vyi479CK06ebfAmJV+hiUlDw8tJ37Wgqa6W8Kt1gjYT
7FQhsf3Vlh67ugNsV9MLIljegEKJXAjDYinTw2Jj5fX0z2Iw7Sq0QQQEkLKtE3qr
GBcaYzFGSrxxAyJ5OfSuTswm9bFuG5/n7McrFVclWvaOmUGkmnzz0GtmzN9fU24u
jnkammWPxNqZlSH/OeyBIvj7Jk+jlk4FhasX/Rp2B547iQEzBBABCAAdFiEEt0gN
15I6LjuDj6/kHb02Ay+x8TIFAmUWu60ACgkQHb02Ay+x8TKckwgAgNsliYdq2THW
zaIu2wG80FRBK8qYmOiL0EfFQg+9n0xNUap4DUcN0iXXkkVA6sOY40wxSLArJAGD
sysR1oVfJgUgelOXWJoFWbv74af1vfr+UosrBrfhhhGA0eA0OL6OAZoY9Cz0XoWq
L6iJc9AU5k68xh+9dQ7VV6j79kF9//BkwZn8utdMeMrhid7s0IhpXh+EJT1A6xqF
3MxztRi/Z49fds2wB4+rp8mqkVLRK0BJFxphNkSOFTdymAFqGcbXTgQL8o6nAgfq
ZPut9xcAkRWDMTu0mkLNi7lt0TcYT45S/7WOXyZ/LnFvNqmHv7wnbUu+nmfvbLdO
q7rf+TA+sLQZRW5CVyBDRVJUIDxjZXJ0QGVuYncuY29tPokCVwQTAQgAQRYhBMGB
Odc0EKIESAAnDsUGC1AD+q4yBQJklV+FAhsDBQkFpPmbBQsJCAcCAiICBhUKCQgL
AgQWAgMBAh4HAheAAAoJEMUGC1AD+q4yYVMP/i1famKribvS9KO+IfAPpnj1IXNQ
bJ4zz1OGBqv1NxEGFKYybuUTKOYQ/8b5UI052O+cqkXd+Y8KW6h6mW4Al6qup4OF
YilamNnVb77T52VjHfXq1mizP6U7JqDVp8tjltuqT8g8asRsEJEn2J744SUDHW63
XbC3T5KjsKsg2UajZwE+YB66hUCS0H6KolOHBb92a+fk9mNGh76660S7fPMJj6wq
hnCdDhpm+DnLHBNT4h/Cm6TB2TMGoLxgJ7AYVdQVPzSffeY7Zyuc8ChvlCedQYjj
EnK42ysLxOk+dTJyYsgNDluW3nCyIcl6DddR/qo2gsowStQNGKZBJ2ZhUIVaLOE4
X2KdNUmFarUnT5+Xb+gmxGnIbc7EJK7NDN1jpRmFxCO5Fn7S/S7Ruu+mXFSpu+yV
8MncZI8wnhDZuSEwPV9HdOJV03IGH3iYIgsSPaRMcgW3Sk6oxj79QUlrFRDFkv1E
bsKDcLL4NopmbGPnuU6/FBjxBKn0qJZSl5vphQuCpSvRa6YG7R6V8OVcBX2Lk7t1
DxhJ3G1atntHr6/sKlozuye61hhm/0pZ3HGun1G1V3akHySPUl8IUZAYJkWOWNqc
8r79MqsTaof20TB0Vb7sHyJQHSo09CTlriYT5MlMOh9r0tQGx24f8BYVbUmV3sB8
viESQRsjbKZriuN4iQIzBBABCAAdFiEEofQdUFX2w/LJAyZLBO3UaGLdMDcFAmSl
zM0ACgkQBO3UaGLdMDcT6w//d7RTS0Yqbap59jREVgCo9cW9ozx+FIt/jnvTWWtX
X25O9z8ngAtbAqrKvAFOHPB0CcVA+hAFtr6QsS5xnWdTET2rp2M0Ohe6xUZhdY8/
1JYCJJEv/nCeyhftAIFg0ALIxYctAPg2QjlGdbu6W4Cv1AnleWqEjrxl0QVfHFCZ
N6+f9h88Yg7ys9q+UDOR+omx9v1VhFBQHF7zOG3wERjNK24R/JeJ4vqHzZRPhePe
vtvTRv5Qsy/Tpkwn9ME03/tlwK1uXZVPR4XpXQR59uGxtgpFqc0Kc15uSfHK7adA
/jidfZDp4mUGw7JBbrDRWeF8T8UvInPhgtavHKQ9BWp7if3deiIEatZqUonMAKAp
jSzkTmR2Cv5c7jI6mdJ2e7/137rgwYMvlXnnxvhbafikS/kjFwWiVLgkZ08UQzPW
MAEFshhwj4q6A6RqhZ/leRCw/M45YD2wfI8QZFgeujtL0Q3eOw2/5hOZZfeGMVER
nk6tYtsNM8S4xg7jLY4m9uoaM4YWxoRMTqF7ol7UtTpOjWDVt8XjGB8e3re1F9lF
S431EMCkeAm9c/wc5np4VtE7OJsB1ez2U8VBb3aVUZ6piCfo5hz9k8be9DvWBFi8
rnKr6zE1MCmBLTKEGOioApcEkximYoOqgOExopSyniWBrIkjwcexgteP+mRr3J1F
T5GJAjMEEAEIAB0WIQSh9B1QVfbD8skDJksE7dRoYt0wNwUCZRa7YQAKCRAE7dRo
Yt0wNxQBD/4irYxU/P4QHsi2KbgwHg/A3VHW3DNPqvYoBY3EZHDDeJv7M364aMQ4
V2pNPSMGUFxe4ik8GRK/8aN9YCOlYJyZt1+MF3u59osW0ij2mT9Nmwl3OaRpo/3O
YZ7B2tgGKfbZmTIbkC3oQP7b7rNu2bn7nXsghN/XxJfmu5GzfGGiFLEMEb/O+Z8m
YNMkKEuWTxG4tOX0Uq+uRwThB6aig8eibd3priPBBZBMNixsmCDpQUTs/5PiYB4P
2H1djtHrGof/vWz+Dd5/UJMf+EdFHJycx/6+i6GvwB8TVkTWCLngfJtZ2zZnY9Q/
kw9wWTsu60YmBHfqnrD3hj/Qw963HWdfWTvwHIr/pEEWETnmqdFdMaCeJqlZcx3l
PO+jC9JNdqzX5UDsOmPbLg/uuHo5WUIPnVaUVo7cNHM8lWviLbs4PCgqH8I0wwnj
kqffrq/Cn4moZ8sgPQd1Pe+FzWjhADpzVC9/RpouweEux/bP4Mai4C6PpbfvIAUr
xN5MsGiFaAqMNMRDUFI0UM7LAISfsWSt1cewwaUrV1v/LWCgh3iJ9gxD1c0n4Bi0
nzqcIKlnzAWZT0/PR3ZQFi36HsZ9EkMHMJAkg/9aJ23ntmV33upPeQfw52D2v7HV
56gVh7es0NfdipbXrFKYJIMDbVztHw4iZOdTNd5zshfbD68GJIkxIYkBMwQQAQgA
HRYhBLdIDdeSOi47g4+v5B29NgMvsfEyBQJlFru/AAoJEB29NgMvsfEyNloH/0+6
iY5p5szp/lM9Dl3G9OEK4dWDZCKQvCHzBndo3ZoxFQcFIjsZGJ8wdjEwS1/8Xr47
dlLFyn5mTLZ5FUV7RwG3je1ZcbVF+osrubm27Nj2MVe5yyr6p/3o9ufvCpxEiZjb
UGS8vgbEbpqo2vh7OjSVO30VAKOhQ26Ih81W/5ABijfqirzjzHSvO27DlOc7dihw
dwvuezM4OuNoIc766nNytfV9j3N6tU9OrnpHq1718CNRmkaTidAsJ/QRO8j7XO+7
SY14wMHDmEDeiqjGTG2gSkYdesurw8KSYD0ZXSRy7i2oqiVa0mHlZCs3RwZYmvTk
lsTMZ5UqLdebJgmQUga5Ag0EZJVfhQEQANMkKS2c9R0bAbGBw93CSdLNx/LTHcbY
OLQJZED8cntntmyW5VaOaaldj2wtNyromSOPkGedifdpByTx3EOqeQg2l6Uc/1oK
FmbnnRp2vlkO0j3ZvlSDKGw3okCIMgFtoawNSkSPzWmKKzKEKfhNnE+YSzDS2z/p
QFS0/VrcT/A0PxDq5yLAwlpPaVLZN3l5n98M+qGDefpIykL4jv9aPLfhW30EKVMF
rwE8s4m/cFukfwY+n8rcda/Zh1N0c50oAirbUdxpVB5pTf1fIASnI+V+NSFfk4Da
/ylRXER4ULsZg3x7uSb4YOFpnW0uPoyKDcR3At398fBt1ZGAXT9qNX5ec7snwvGA
8U8p7ezL3tr1TkG8yqKj9cRl4naqJD7N+rPOuTe6A1ygCNZozlXnPmxDx1313cC2
QHqNHCuAARJc7CzSu7TY8A7E7pYmJgLtkXGKOT4WULXWgWg11B8o3yK5SNGnoeQN
B3S5DVjsHjuC02Bb6R63kgZbA0C/3jJ6E1GvraGFMSpetKA3iIR7ofafl9DL8DBL
uhrc2t0fXrjl8R+pWCA6AU1b0S/hGOrYt1B/fnRaa9Xber6teA3iCjRthYaCXdSc
EXdWwI77Hn8IpeLu8bCliMrCl1r78QzS2muVSI8kgxYs+6FTmrytHwr/waglzxBo
qRlRsxPvrlR3ABEBAAGJAjwEGAEIACYWIQTBgTnXNBCiBEgAJw7FBgtQA/quMgUC
ZJVfhQIbDAUJBaT5mwAKCRDFBgtQA/quMgI3D/0Xp3xkQo2DbLp0zaoOmde29mWB
ctJNPZ6LBt0P3cvWwJWksYsWu6AUUzdKwTth5CHB75adYhmWGY80MbloG3L7fZFk
SXG0aiLuSZkCqqKiHqDARkz0AOzh9QBS9APG1zk1gKUkjG5dhtAm/C+0K3aestd1

```
PjwGGvT1Td6KFI4+ynr1Q0L56sQZVz/eoHAg+zw/JrixRuxhbygV6BiEQqRC+MJv
LC6dHaHW1kxSvwRRdOmmDxb11ObMC8QH0HSsVZcSiVZRPC8GgGCtJdA+yujxmKKQ
TwCxSun8eCLuhk+V4j6+r/kkJKV/THHnExE7grMtmlN53IupeTXHNhqwZhWWpUwc
68ARhW3We0teK6D1n0Es5BzapTyT2IbFOe2fJuEHfBcU3F5SRCnSCHRlZ09gVWMJ
mFr6glv7u5UY53BGOsIq15ASaT1QKAuFVWRu8Ib551TgkvIwRvJwMl7Udlc/Ek2r
eatRxvwNHZFO/j8OiCvlXwJmpgANS0gimqk1Iw4YfLTfhCR8DTl5bJJMV7ohUJM6
KWsI1zee2c4/LttrbUB/z+yilioUXhUoQUu2zXfgogKuShQMU26GH7UQAu2VL1dd
edf/Wn7XpCM1Rx8oq01H+FMWfqw8w+0xZDP34+1Csf4mSsXajdbhyqo44OjSYKsO
rxRk6ih2wAnMMv6MEg==
=VWYP
-----END PGP PUBLIC KEY BLOCK-----
```

The key and its signature are available on the EnBW-CERT website:
https://www.enbw.com/cert

In addition, the PGP key is also published on the usual public key servers and can be downloaded from there:

- OpenPGP public key server (http://pgpkeys.mit.edu)
- PGP Global Directory (https://keyserver.PGP.com)

EnBW-CERT attempts to collect as many signatures as possible from other teams or individuals for the public EnBW-CERT key to strengthen the PGP "Web of Trust."

1.9 Members of EnBW-CERT

The members of the EnBW-CERT are listed here:

- Julia Becker
- Jörg Doll
- Christoph Matthäus (Team Coordinator)
- Sophia Matthis
- Hanno Nofkin
- Sergey Levin
- Simon Schäfer
- Ulrich Stadie (Backup Team Coordinator)
- Dominik Weber
- Marco Wiehr

Team coordinator Christoph Matthäus is the nominated Information Security Manager for the EnBW IT department and responsible for the management and control of the EnBW-CERT at EnBW Energie Baden-Wuerttemberg AG, as well as the role of liaison officer.

1.10 Hours of Operations

The regular business hours of the EnBW-CERT are normally Monday to Friday from 09:00–17:00 (except on public holidays).
In addition, EnBW-CERT is on standby 24/7 throughout the year for EnBW, which can be reached via the EnBW alarm channels.

1.11 Additional Pieces of Information

General information on EnBW-CERT is available on the EnBW-CERT website:
https://www.enbw.com/cert/

EnBW-CERT is a member of the following organizations:
- CERT-Verbund
  http://www.CERT-verbund.de

EnBW-CERT strives for membership in the following organizations:
- TF-CSIRT Trusted Introducer (TI)
  http://www.trusted-introducer.org/directory/teams/cert-bund.html
- FIRST (Forum for Incident Response and Security Teams)
  http://www.FIRST.org/members/teams/cert-bund

1.12 How to reach us

EnBW-CERT monitors its contact e-mail address CERT@enbw.com.
In addition, the EnBW-CERT also monitors the official abuse e-mail contact address abuse@enbw.com.

In urgent cases, [important] can be included in the subject line to indicate the urgency of an e-mail. For encrypted communication, the EnBW-CERT provides its PGP key and S/Mime certificate (see 1.8).

In critical cases, contact can also be made around the clock via the on-call hotline.
In addition, all tickets of the EnBW IT ticketing system declared as security incidents are brought to the attention of the EnBW-CERT and taken care of by the EnBW-CERT on-call officer.

2 Statute

2.1 Mission Statement

As part of EnBW's information security process, the EnBW-CERT acts as a point of contact for IT security incidents in the provision of IT services and processes. It also offers certain services for critical infrastructures.

The objectives of the EnBW-CERT are:
- to support EnBW in the event of computer security-relevant incidents as part of reactive measures and
- support the processes/members of EnBW in implementing initiative-taking measures to reduce the risk of such accidents.

2.2 Area of Responsibility / Constituency

The area of responsibility ("Constituency") of EnBW-CERT is the entire EnBW Group, as described in the context of the following guidelines:
- "EnBW Group Policy on Information Security"
- "FE IT Information Security Guideline"

These two policies are referred to as "EnBW Information Security Policies" in the following.

The EnBW-CERT is responsible for the following autonomous system:
- AS15698

2.3 Organizational Localization and Funding / Membership

EnBW-CERT has been appointed as the information security team for EnBW. Organizationally, the EnBW-CERT is established in the functional unit IT (FE IT) and is also financed via IT.

The EnBW-CERT has set itself the goal of establishing links to various industrial and academic CSIRTs throughout Germany as well as to international CSIRTs as required.
EnBW-CERT is a member of the German CERT Association and aims to establish a membership of TF-CSIRT/Trusted Introducer (TI) and FIRST (Forum of Incident Response and Security Teams) for the future.

2.4 Commissioning and Authorization

The EnBW-CERT processes on behalf of and with powers delegated to the EnBW-CERT by the head of the functional unit IT (C-TI) and the CIO of EnBW for the performance of its tasks, for hazard prevention. Further information on the mandate and authority of the CIO can be found in the "EnBW Information Security Policy".

EnBW-CERT strives to cooperate with system administrators and users in the best conceivable way to achieve EnBW's security objectives, but also makes use of authority to issue instructions if necessary.

Employees and affiliated partners of the EnBW community who wish to lodge a complaint against the actions of the EnBW-CERT should contact the Head of the "EnBW IT Cybersecurity". If the clarification achieved as a result is not satisfactory, this can be brought to the attention of the CIO of EnBW for information and possible further appreciation.

2.5 Network Ranges in Responsibility of EnBW-CERT

The following public IPv4 networks are in responsibility of EnBW-CERT:

- Autonomous System AS15698: 195.35.72.0/21

The following public IPv6 networks are in responsibility of EnBW-CERT:

- 2a0b:cfc0:6000::/44
- 2a0b:f400::/32
- 2a0d:5840::/44
- 2a0d:5840:80::/44
- 2a0d:5840:c080::/41
- 2a0d:5840:ff80::/41

In addition, the EnBW-CERT is also available on various cloud-based networks of EnBW of various cloud service providers (e.g., AWS, Azure, Google) if EnBW uses them.
The various private networks operated by C-TI for EnBW are also the responsibility of EnBW-CERT.

3 Policies and Regulations

3.1 Classification of Incoming Information

All incoming information is classified and treated as confidential or higher. This strict classification system prevents the unintentional disclosure of information classified by other (external) classification systems that may not correspond to those of EnBW-CERT.

Regarding the transfer of confidential information, EnBW-CERT follows the Traffic Light Protocol (TLP; developed by FIRST; https://www.first.org/tlp/). Information received by the EnBW-CERT that is classified according to TLP is treated confidentially according to the classification.

Electronic information is usually only stored on encrypted storage media. EnBW-CERT members only perform key management of these tasks.

3.2 Retention of Records

The systems and data carriers used by EnBW-CERT (personal computers, forensic systems, archive, and transfer data carriers) are always basically encrypted.
The data records containing information on security incidents are kept in encrypted form at least for the duration of the ongoing investigation and any legal proceedings. This applies to records that are stored either electronically or as a hard copy. These data records are only deleted when the incident processing has been completed and there are no further retention requirements (e.g., ongoing legal proceedings or retention periods).
Electronic information is stored in a central database of the "BaseIT" ticketing system of EnBW IT. This database can only be accessed via authenticated and secured connections. Encrypted backups of this database are created daily and stored in the backup systems provided by EnBW IT.
Paper records of the EnBW-CERT (e.g., handover reports, final reports) are stored in the EnBW-CERT's access-secured premises in lockable cabinets that are only accessible to EnBW-CERT employees.
Classified reports can be compiled and printed for authorized individuals. Reports cleaned of sensitive information and unclassified reports can be created and published for training purposes.

3.3 Deletion and Disposal of Data Storage Devices and Recordings

Media such as hard drives, floppy disks or flash drives are deleted in accordance with the guidelines of the Federal Office for Information Security (BSI) as part of disposal by EnBW-CERT before they are handed over for physical disposal. All deletion actions of media that belong to the EnBW-CERT are recorded in a log file and are only conducted by EnBW-CERT employees.
The deletion/destruction of optical media is done by physical destruction, either manually or with a special shredding machine.
To delete paper records, they are either destroyed manually or handed over to a service provider certified in accordance with DIN 66399 using special containers for disposal. The data carriers (after they have been deleted by EnBW-CERT) are also handed over to the service provider for disposal in accordance with DIN 66399.

3.4 Incident Types and Support Levels

EnBW-CERT is entitled to address all types of IT security incidents that occur within and against the area of responsibility of EnBW-CERT.
The level of support provided by EnBW-CERT to data subjects varies depending on the nature and severity of the incident or problem, the area affected, the size of the affected user community and the EnBW-CERT resources available at that time, although an answer is provided in all cases. Resources are allocated according to the following priorities, which are listed in descending order, if necessary, after triage by EnBW-CERT:

1. Threats to the physical security of people.
2. Root or system-level attacks on any central IT management system or part of the backbone network infrastructure (onprem and cloud).
3. Root or system-level attacks on relevant publicly accessible systems (for multi-user or dedicated purposes) (onprem and cloud).
4. Risk of restricted confidential service accounts or software installations (onprem and cloud).
5. Denial-of-service attacks on one of the above systems (onprem and cloud).
6. Large-scale attacks of any kind, e.g., sniffing/recon attacks, social engineering attacks or attacks on passwords/login interfaces (onprem and cloud).
7. Threats, harassment, or other criminal offences affecting individual user accounts.
8. Risk to individual user accounts on multi-user systems.
9. Compromised personal computer systems.
10. Falsifications, misrepresentations or other security-related violations of local rules and regulations, e.g., email manipulation or unauthorized use of IRC bots.
11. Denial of service attacks on individual user accounts, e.g., Mail bombardments.

Incidents other than those mentioned above are prioritized according to their severity, impact, and prevalence.
End users are not directly supported. They are expected to contact their respective system administrators, network administrators, information security managers (ISM) or department heads for assistance. The EnBW-CERT will support the two latter groups of persons.
The EnBW-CERT attempts to meet the various levels of expertise of the persons involved by providing specific information and support to target groups. No training or system maintenance can be conducted by EnBW-CERT as part of incident processing.
In most cases, the EnBW-CERT will provide the necessary instructions and pieces of information for the implementation of suitable measures. Additionally, the provided instructions and pieces of information should enable the involved persons to derive a need for further necessary training.

EnBW-CERT endeavors to keep the established contact persons in the EnBW (EnBW Information Security Community) informed of potential serious vulnerabilities and will proactively inform this community of such vulnerabilities whenever possible and whenever EnBW-CERT deems it appropriate. However, this does not release the system administrators from their responsibility to take care of the security of their systems.

3.5 Collaboration, Interaction and Disclosure of Information

Although there are legal and ethical restrictions on the flow of information from the EnBW-CERT, which are also listed in the "EnBW Information Security Policy" and which are all complied with, EnBW-CERT declares its intention to contribute to the spirit of cooperation created by the Internet.
Therefore, while the EnBW-CERT acts appropriately to protect the identity of members of the area of responsibility and other data subjects where necessary, information is otherwise freely exchanged to support others in resolving or preventing security incidents.

In the following paragraphs, "affected parties" refers to the legal owners, operators, and the corresponding IT systems. It does not refer to unauthorized users, including otherwise authorized users, who use a facility in an unauthorized manner; such intruders cannot expect confidentiality from EnBW-CERT. Existing legal rights to confidentiality, which such an intruder may or may not have, constitute an exception to this. These are of course respected where they exist.

Information considered for publication is classified as follows:

1. Private user information is information about specific users or, in some cases, specific applications that must be considered confidential for legal, contractual and/or ethical reasons. Private user information is not published in identifiable form outside the EnBW-CERT, unless provided for below. If the user's identity is or has been made unrecognizable, the information can be shared, for example to show a sample file as it was modified by an intruder or to demonstrate a specific social engineering attack.

2. Intruder information is like private user information but relates to intruders. While intruder information, in particular identifying information, is not disclosed to the public (unless it becomes publicly accessible, e.g., because criminal charges have been filed), these can be exchanged with affected system administrators and CSIRTs as part of incident handling.

3. Private website information is technical information about certain systems or websites. These are not released without the permission of the owners of the relevant website, except as provided below.

4. Vulnerability information is technical information about vulnerabilities or attacks, including patches and workarounds. Information about security vulnerabilities is published freely, although every effort is made to inform the respective provider before it is disclosed to the public ("responsible disclosure").

5. Unpleasant information includes the statement that an incident has occurred, as well as information about its extent or severity. Unpleasant information can relate to a website or a specific user or user group. Unpleasant information will not be published without the permission of the relevant website or users, except as provided below.

6. Statistical information is unpleasant information, whereby the identifying information is removed. Statistical information is published at the discretion and in consultation with the head of C-TI.

7. Contact information is information that enables internal and external system administrators and CSIRTs to be reached. Contact information is published freely if necessary or appropriate (e.g., in the context of an incident), unless the contact person or institution has requested that this not be the case or if EnBW-CERT has reason to believe that the dissemination of this information would not be valued.

Potential recipients of information from the EnBW-CERT are classified as follows:

1. Members of the EnBW Supervisory Board, the EnBW Board of Management, members of the Legal Department, the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) have the right to receive all information requested by them on an IT security incident (or related questions) that has been submitted to them for processing.

2. Due to their responsibility and the resulting expectations of confidentiality, members of C-TI management at L1 level or higher have the right to receive all necessary information to enable the handling of IT security incidents in their respective area of responsibility.

3. Members of the EnBW Corporate Security department and the EnBW-CERT are entitled (if their participation in an investigation of an information security incident has been requested or if such an investigation has been initiated at the request of EnBW Corporate Security or the EnBW-CERT) to request all necessary information in order to enable investigations to be carried out and incidents to be processed in their area of responsibility.

4. System administrators of EnBW or EnBW IT receive confidential information as far as this is necessary for their support in an investigation or to secure their own systems.

5. Members of EnBW have a right to information relating to the security of their own computer accounts, even if this means that "intruder information" or "unpleasant information" is disclosed about another user.
   Members of EnBW are entitled to be notified if they suspect that their account has been compromised.

6. EnBW customers or external parties are not entitled to request and receive information directly from EnBW-CERT. Information is transferred to customers or third parties by the legal department or, in the case of customers, by the customer interface (CRM). After checking the lawfulness of the data disclosure, EnBW-CERT will compile the required information and provide it in accordance with the instructions.

7. In general, members of the EnBW-CERT area of responsibility do not receive restricted information unless the parties concerned have given permission to disseminate the information.

   Statistical information can be made available to the members of the area of responsibility.
   EnBW-CERT is not obliged to report all incidents to the Community, even if it can decide to do so. It is likely that the EnBW-CERT will either inform all directly affected parties of the way in which they are affected or encourage the affected website to do so.

8. In general, no restricted information is made available to the general public. This means that no effort is made to communicate with the public. The EnBW-CERT therefore treats any information disclosed by the EnBW-CERT to members of EnBW as if it were disclosed to the general public and therefore adapts the information accordingly.

9. The IT security community is treated in the same way as the general public. Members of the EnBW-CERT can and will participate in discussions within the IT security community (e.g., newsgroups, mailing lists (including complete disclosure lists such as bugtraq) and conferences). In doing so, they will treat the information disclosed to these circles as if it were made public. While technical topics (including weaknesses) can be discussed at any level of detail, all examples originating from within the area of responsibility of the EnBW-CERT are corrected in such a way that it is not possible to identify the affected parties.

10. The press is also considered part of the general public. EnBW-CERT will not interact directly with the press in relation to IT security incidents, except to refer to information that has already been provided by EnBW to the general public. All inquiries relating to information security incidents are referred to the EnBW Press Department.
    If necessary, information is compiled and prepared by EnBW-CERT and then made available to the responsible departments of EnBW for press work or customer relationship management.
    Irrespective of the above restrictions, the members of the EnBW-CERT may, in consultation with the press office of EnBW, give interviews on general computer security issues; indeed, they are also encouraged to do so as part of the EnBW self-image.

11. In some cases, confidential information is shared with external entities and other CSIRTs as part of IT security incident investigations. This is only done if the trustworthiness and legitimate interest of the external bodies can be verified. The information transmitted is limited to the extent that it is helpful in the investigation of an incident. The exchange of such information is with known CSIRTs (e.g., CERT-BUND).
    To resolve a security incident, otherwise semi-private but harmless user information such as the origin of connections to user accounts is not considered extremely sensitive and can be transferred to a third party with usual precautions. "Intruder information" is freely transmitted to other system administrators and CSIRTs. "Painful information" may be disclosed if there is reasonable assurance that it will remain confidential and if it is necessary to resolve an incident.

12. Manufacturers are considered foreign CSIRTs for most purposes. EnBW-CERT wants to encourage providers of all types of networks and computer equipment, software, and services to improve the security of their products. For this purpose, a security vulnerability detected in such a product, together with all technical details necessary to identify and resolve the problem, shall be reported to the manufacturer.
    Identifying details will not be communicated to the manufacturer without the approval of the affected parties who have discovered the vulnerabilities.

13. The law enforcement authorities will receive due cooperation from EnBW-CERT, in accordance with the EnBW guidelines and all relevant laws, including all information they need to investigate. The coordination of this cooperation is managed by the legal department of EnBW. The requested information will be made available to the Legal Department by EnBW-CERT. The Legal Department will provide the information to the law enforcement authorities.

3.6 Communication and Authentication

Given the types of information that the EnBW-CERT is likely to deal with, phones are considered sufficiently secure to be used even if they do not offer encryption of the voice stream.
Unencrypted e-mails are not considered particularly secure but are only sufficient for transferring data with low sensitivity. If it is necessary to send extremely sensitive data by e-mail, PGP, GPG or S/MIME as well as other security methods (e.g., Microsoft Information Protection MIP) are used depending on availability.
Network file transfers are considered as e-mail for these purposes: Sensitive data is encrypted for transmission and attention is paid to encryption of network communication.

If it is necessary to establish a relationship of trust with a previously unknown counterparty (e.g. before EnBW-CERT can take action on the basis of information from the counterparty or before EnBW-CERT discloses information to the counterparty), both the identity and the trustworthiness of the unknown counterparty are checked until an appropriate level of trust has been established.
Within EnBW and with known external bodies, recommendations from known trustworthy persons are sufficient to authenticate someone and thereby establish the necessary level of trust. Otherwise, appropriate methods are used (e.g., search for FIRST members, use of WHOIS and other internet registration information, together with a phone call back or contact verification by means of signed email) to ensure that the requesting counterparty is trustworthy.
Data that is transmitted to EnBW-CERT by e-mail and that must be trusted is checked by EnBW-CERT by contacting the sender personally or by means of digital signatures (PGP/GPG/S/MIME).

4 Service Offer

4.1 Reactive Measures for IT Security Incidents

EnBW-CERT supports those responsible and their system administrators in the operational processing of the technical and organizational aspects of IT security incidents within the area of responsibility of EnBW-CERT.
The EnBW-CERT provides support, assistance, and advice in the following phases of incident management:

4.1.1 Triage

- Investigate whether a security incident has occurred.
- Determine the extent of the incident.
- Decision on the procedure for managing the incident.

4.1.2 Coordination of Incident Response Measures

- Identify the original cause of the incident, i.e., identifying the vulnerability exploited by the attacker.
- Support in contacting/delegating to other external entities that may be involved.
- Support in contacting/delegating to internal EnBW departments (e.g., Group Security, Legal Department, Data Protection Officer) and/or the relevant law enforcement authorities, if applicable.
- Create reports to other CSIRTs.
- Write notifications to affected users, if applicable.

4.1.3 Handling of Incidents

- Support/consultancy to resolve the vulnerability, if possible.
- Securing the system from the impact of the incident.
- Assess whether certain measures produce sufficient results in relation to their costs and risks, especially for measures aimed at potential prosecution or disciplinary action, such as collecting evidence after an IT security incident, observing an incident in progress, using honeypots.
- Gathering evidence where criminal prosecution or disciplinary action is considered.

In addition, the EnBW-CERT collects statistics on incidents that occur within or affect the defined area of responsibility and informs the members of the area of responsibility if necessary to help protect against known attacks.
In order to request the services of EnBW-CERT in the event of an incident, support should be requested by opening a security incident or via IT Support or the Service Cockpit (see Section 1.4) or via the EnBW-CERT e-mail address (see Section 1.12) if EnBW-CERT has not yet contacted you. It should be noted that the available support varies according to the specifications and priorities described in section 3.4.

4.2 Proactive Measures

EnBW-CERT coordinates and offers the following services, depending on the available resources ("best effort").

4.2.1 Provision of Information and Situational Pictures

- Distribution of EnBW-relevant safety information from monitored sources for information security and vulnerability alerts (e.g., BSI/US-CERT/US-CISA recommendations, published safety information from manufacturers).
- EnBW-CERT obtains threat information from various sources and evaluates it. In the event of relevance for the constituency of the EnBW-CERT, the EnBW-CERT publishes corresponding safety information via internal communication channels and processes.
- In addition, EnBW-CERT uses the threat information available to it to create a current threat situational picture. This is incorporated into the reports of the EnBW-CERT and is also used for other measures, e.g., the prioritization of measures to prepare for hazard prevention.
- While the records of IT security incidents remain confidential, statistical reports are regularly made available to interested and authorized bodies at EnBW for the purpose of evaluating and improving IT security measures.

4.2.2 Operation of the Phishing Mailbox

- EnBW-CERT operates the phishing message box (phishing@enbw.com). EnBW members can send suspicious emails to this address, which are then analyzed by EnBW-CERT. The reporter is then notified accordingly. Lessons learned are used by EnBW-CERT to improve corresponding processes, identify training needs, or provide corresponding security information to the EnBW community via corresponding channels (e.g., due to a phishing campaign currently running against EnBW).

4.2.3 Education/Training

- The members of the EnBW-CERT consistently offer training on IT and information security topics. These training courses are primarily aimed at EnBW IT employees and, if capacities or requirements exist, also at EnBW as a whole.

4.2.4 IT Security Audits

- Perform vulnerability scans: The EnBW-CERT can perform its own vulnerability scans or access the results of the centrally performed vulnerability scans to check dedicated systems for vulnerabilities if necessary and to be able to initiate countermeasures at an early stage.
- Conducting IT security audits: Information associations and the services provided by them (if they are part of the networks defined in Section 2.5) that fall within the area of responsibility of EnBW can be audited to determine their current maturity level regarding IT and information security. This information on the maturity level of the security level is made available to interested and authorized parties at EnBW to facilitate the integration and use of the services provided. However, details of the safety analyses will be treated confidentially and only made available to the affected parties.
- Records of handled security incidents are kept in accordance with the regulations listed in sections 3.2/3.3.
  While the records remain confidential, statistical reports are regularly made available to interested and authorized bodies at EnBW.

4.3 Additional Services

4.3.1 Communication with External Bodies

- The EnBW-CERT is the designated point of contact for communications with the German Federal Office for Information Security (BSI) and as the reporting body for KRITIS reports. For this reason, the EnBW-CERT is responsible for coordinating and issuing corresponding notifications.
- The EnBW-CERT is also responsible as a point of communication with the cyber insurer for reporting (possibly) incurred damage and for further coordination as part of the incident handling of the insurance claim.
- Point of contact for reporting vulnerabilities by third parties to EnBW-CERT as well as communication and coordination with the reporting third parties and relevant bodies to remedy them.

4.3.2 Consulting on Information Security Issues

- The members of the EnBW-CERT conduct consultations on projects in the planning stage and on established services on aspects of IT and information security as well as to a certain extent on technical data protection requirements. In the case of more complicated data protection issues, the data protection officers are involved.

5 Incident Reporting Forms

Incidents can be reported to EnBW-CERT via any communication channel (in accordance with Chapter 1) and do not have to take any special form.

6 Exclusion of Liability

While every precaution is taken in the creation of information, notifications and warnings, EnBW-CERT assumes no responsibility for errors or omissions or for damages resulting from the use of the information contained therein.