Acceptable Use Policy

This MYNXG Acceptable Use Policy (hereinafter referred to as “AUP”) provides a description of the prohibited uses of the MYNXG Solution and/or MYNXG Platform and related Digital Products and Digital Services (hereinafter referred to as “Service Offerings”) provided by MYNXG as the IoT Provider.

1 NO ILLEGAL, HARMFUL OR OFFENSIVE CONTENT

1. You and your End Users shall not use, or encourage, promote, facilitate, or instruct others to use the Service Offerings for any illegal, harmful, or offensive use, or to transmit, store, display, distribute, or otherwise make available content that is illegal, harmful, or offensive.
2. Prohibited activities include, but are not limited to, the following:
    a. any activities prohibited by any law, regulation, government order, or decree, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting, or facilitating child pornography;
    b. any activities where the cryptographic and or machine learning capabilities of the MYNXG Solution and/or MYNXG Platform, and Service Offerings are used for military, cybercrime, virtual currency mining, gambling including but not limited to online gambling, lotteries, raffles, sports forecasting and odds-making;
    c. any activities, prohibited by the law of the Federal Republic of Germany and any rules set forth versus Nazi Content like flags, symbols, statement and any kind of racism content or propaganda;
    d. activities that may be harmful to others, our operations, or our reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (for example, get-rich-quick schemes, Ponzi or pyramid schemes, phishing, or pharming) or engaging in other deceptive practices;
    e. content that infringes or misappropriates the intellectual property or proprietary rights of others;
    f. content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable; and
    g. content or other computer technology that may damage, interferes with surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, or other malware.

2 NO SECURITY AND SAFETY VIOLATIONS

1. You and your End Users must comply with, and may not work around, any technical limitations in the Service Offerings that only allow you or your End Users to use the MYNXG Solution and/or MYNXG Platform, Digital Product and Digital Service Offerings in certain ways.
2. You and your End Users may not download or otherwise remove copies of software or source code from the Service Offerings unless explicitly authorized.

3. You and your End Users may not tamper with, not open, disassemble, bend, deform, puncture the Digital Products (including but not limited to Supplier Hardware, MYNXG Gateway, Thing and Sensor Hardware) and expose such Digital Products to fire, explosion or other hazard, as such Digital Products may contain lithium batteries.
4. You and your End Users may not use the MYNXG Solution and/or MYNXG Platform and Service Offerings to violate the security or integrity of any network, computer, or communications system, software application, or network or computing device (each a "System").
5. Prohibited activities include, but are not limited to, the following:
    a. accessing or using any MYNXG Solution and/or MYNXG Platform and its sub-Systems without permission, including attempting to probe, scan, or test the vulnerability of a MYNXG Solution and/or MYNXG Platform or to breach any security or authentication measures used by a MYXNG Solution and/or MYNXG Platform sub-System;
    b. monitoring of data or traffic on the MYNXG Solution and/or MYNXG Platform without permission; or
    c. forging MYNXG Secret and Value Date, MYNXG Blockchain, API based communication, packet headers, email headers, or any part of a message describing such message's origin or route. This prohibition does not include the use of aliases or anonymous remailers.

3 NO NETWORK ABUSE

1. You and your End Users may not use the MYNXG Solution and/or MYNXG Platform, and Service Offerings to make network connections to any users, hosts, or networks unless you or such End User has permission to communicate with them.
2. In particular, MYNXG Solution and/or MYNXG Platform and Services Offerings are prohibited to be used towards 3rd party system or being exposed by 3rd party systems by the following activities:
    a. monitoring or crawling, of another System that impairs or disrupts the System being monitored or crawled;
    b. creation of denial of service attack deliberate or accidental towards or from another System in a way that
    c. communication procedures cannot respond or responds so slowly that it becomes ineffective;
    d. irregular mail usage or service attempts including any to overloading by mail bombing, news bombing, broadcast attacks, or flooding techniques;
    e. operating network services like open proxies, open mail relays, or open recursive domain name servers; or
    f. using manual or electronic means to avoid any use limitations placed, such as access and storage restrictions

4 NO MESSAGE ABUSE

1. You and your End Users shall not distribute, publish, send, or facilitate the sending of unsolicited mass emails, messages, promotions, advertising, solicitations, or other spam, including commercial advertising and informational announcements.
    g. You and your End Users shall not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission.

5 NO INTELLECTUAL PROPERTY AND EXPORT CONTROL VIOLATIONS

1. You and your End Users shall not sublicense, distribute, create derivative works of, or reverse engineer any of the MYNXG Solution and/or MYNXG Platform, or authorize any third party to do so.
2. MYNXG shall retain rights to all MYNXG Intellectual Property, Intellectual Property Rights and Supplier Content and all rights to MYNXG Solution and/or MYNXG Platform, all modifications or improvements to the source code of the MYNXG Solution and/or MYNXG Platform, no matter which Party made such improvements or modifications to the source code.
3. You and your End Users will be responsible for complying with all applicable laws and regulations, including but not limited to export control laws, using the MYNXG Solution and/or MYNXG Platform. Specifically, you and your End Users agree that the MYNXG Solution and/or MYNXG Platform is not being or will not be shipped, transferred or re-exported, directly or indirectly, into any country prohibited by the United States Export Administration Act and the regulations thereunder, or will not be used for any purposes prohibited by such Act. Specifically, the export restrictions of the U.S. Department of State, Country Policies and Embargoes in particular, the requirements regarding Telecommunications and "Information Security" are applied, as well as the export classification numbers for products of the U.S. Bureau of Industry and Security (BIS) regarding the U. S. Commerce Control List ECCN (Category 5) Telecommunications and Information Security are applied.

6 NO HIGH RISK SYSTEMS AND AREAS

1. You and your End Users:
    a. will not use the MYNXG Solution and/or MYNXG Platform for the operation and /or control of or use within a High Risk System, if the functioning of such a High Risk System is dependent on the MYNXG Solution and/or MYNXG Platform.
    b. not to use and operate the MYNXG Solution and/or MYNXG Platform within High Risk Areas unless the MYNXG Solution and/or MYNXG Platform has been explicitly been designed, certified, marked accordingly for the use by the MYNXG, in such High Risk areas.
    c. Where High Risk System shall mean a device or system that required enhanced safety functionalities such as fail-safe or fault-tolerant features to maintain a safe state where its reasonably foreseeable that failure of the device or system could lead to direct death, personal injury or catastrophic property damage. Without limitation, High Risk Systems may be required in the critical infrastructure, direct heal support, aircraft, chemical production, navigation systems, communication systems, transport facilities, weapon systems, military or aerospace applications.
    d. Where High Risk Area shall mean a device or system that is required to operate in an environment with hazardous, explosive, or otherwise dangerous materials, including but not limited to materials that are subject to the ATEX, IEX, NFPA, NEC 500 and NEC 505 directives or equivalents
2. You and your End Users are solely responsible for, and bears all risks associated with such controlling and operating such High Risk Systems and/or High Risk Areas.

7 MONITORING AND ENFORCEMENT

1. We reserve the right, in our sole discretion, to investigate any violation of this AUP or any misuse of the Service Offerings by you, your End Users, or any third party.

2. We may, in our sole discretion, remove, disable access to, or modify any content or resource that violates this AUP, the Agreement, or any other agreement with you related to the MYNXG Solution and/or MYNXG Platform and Service Offerings.
3. You and your End Users shall not block or interfere MYNXG, or any third party on MYNXG's behalf, in monitoring of usage of the MYNXG Solution and/or MYNXG Platform for building, operating and servicing the MYNXG Solution and/or MYNXG Platform as well as MYNXG's internal purposes, including but not limited to security, availability, compliance, billing, reporting purposes and improvement purposes.
4. We may report any activity that we, in our sole discretion, believe to be in violation of any law or regulation to law enforcement officials, regulatory bodies, or other appropriate third parties. Our reporting for such purpose may include disclosing appropriate End User or account information. Such reporting may also include providing network and systems information related to violations of this AUP.
5. You and your End Users shall comply with any license limitation relevant for MYNXG Solution and/or MYNXG Platform, including but not limited to user limits, copy limits, processor limits, data limits, communication cost limits, or restrictions to designated computers, locations or facilities.
6. You and your End Users shall not block or interfere MYNXG, or any third party on MYNXG's behalf, in monitoring of usage of the MYNXG Solution and/or MYNXG Platform for building, operating and servicing the MYNXG Solution and/or MYNXG Platform as well as MYNXG's internal purposes, including but not limited to security, availability, compliance, billing, reporting purposes and improvement purposes

8 REPORTING.

Digital Millennium Copyright Act (DMCA) Notice

1. If you become aware of any violation of this AUP, you must promptly notify MYNXG and provide us with any requested assistance to mitigate, stop, or remedy such violation.
2. To report any violation of this AUP, or to otherwise contact us with respect to acceptable uses of the Service Offerings, you may use the following contact information: by email to info(at)mynxg.com
3. You are responsible for responding within a reasonable timeframe to any request from any third party regarding your or any End User's use of the MYNXG Solution and/or MYNXG Platform and Service Offerings, such as a request to take down content under the U.S. DMCA (DMCA) or other applicable laws. We reserve the right to take down content hosted by us in order to comply with the safe harbor requirements of the DMCA or for any reason permitted by the Agreement or required by law. If you wish to provide us with a counter notice, you may notify us in accordance with the counter notice provisions of the DMCA at the above email.

9 GENERAL.

1. Examples described in this AUP are not exhaustive.
2. We may modify this AUP at any time by giving notice to you or by making such modifications available as part of the MYNXG Solution and/or MYNXG Platform and Service Offerings.
3. You shall comply with, and shall cause End Users to comply with, this AUP.