contact@brandnetz.eu
+494088358374

Vertraulichkeitsvereinbarung

ZWISCHEN:

Brandnetz EU, vertreten durch den rechtlich verantwortlichen Betreiber:

Dario Nüssler Straße der Völkerfreundschaft 7 Deutschland - 17192 Klink	Pascal Röse Am Exerzierplatz 13 Deutschland - 21073 Hamburg

(nachfolgend „Brandnetz“)

UND:

Vorname	Nachname
Straße	Hausnummer
Ort / PLZ	Land

(nachfolgend „Teammitglied“)

wird für die Stelle **„Community Administrator (m/w/d)“** hiermit folgende Vertraulichkeitsvereinbarung (nachfolgend „Vereinbarung“) geschlossen:

§ 1 – Gegenstand und Zweck

Diese Vereinbarung regelt den vertraulichen Umgang mit nicht öffentlichen Informationen, die dem Teammitglied im Rahmen seiner Tätigkeit oder einer geplanten Tätigkeit für Brandnetz zugänglich gemacht werden.

1. Sie gilt insbesondere für Tätigkeiten in folgenden Bereichen:
   - Community-Management und Moderation
   - Administration und Projektleitung
   - Softwareentwicklung und technische Betreuung
   - Minecraft-Server und zugehörige Plugins
   - Discord, Forum und andere Kommunikationsplattformen

Vertraulich

- Brandnetz Manager und interne Verwaltungssysteme
- Support, Organisation und Projektentwicklung

2. Ziel dieser Vereinbarung ist der Schutz berechtigter Vertraulichkeitsinteressen von Brandnetz sowie der personenbezogenen Daten seiner Mitglieder, Teammitglieder und sonstigen betroffenen Personen.
3. Diese Vereinbarung begründet für sich genommen weder ein Arbeitsverhältnis noch eine Verpflichtung zur Erbringung bestimmter Arbeitsleistungen. Bestehende gesetzliche oder anderweitig vertraglich vereinbarte Rechte und Pflichten bleiben unberührt.

§ 2 – Vertrauliche Informationen

1. Als vertraulich gelten nicht öffentlich zugängliche Informationen, deren Geheimhaltung von Brandnetz ausdrücklich verlangt wird oder deren Vertraulichkeit sich aus ihrer Art oder den Umständen der Offenlegung ergibt.
2. Hierzu gehören insbesondere:
    1. **Technische Informationen**
        - Nicht veröffentlichter Quellcode, Softwarearchitekturen und interne Dokumentationen
        - Datenbankstrukturen, Serverkonfigurationen und Infrastrukturpläne
        - Zugangsdaten, API-Schlüssel, Tokens und kryptografische Geheimnisse
        - Interne Sicherheitskonzepte und nicht öffentlich bekannte Schwachstellen
        - Unveröffentlichte Funktionen, Entwicklungen und Projektpläne
    2. **Organisatorische Informationen**
        - Interne Teamgespräche, soweit diese vertrauliche Inhalte betreffen
        - Nicht veröffentlichte Entscheidungen und Strategien
        - Interne Bewerbungs- und Personalangelegenheiten
        - Vertrauliche Vertrags- und Geschäftsinformationen
        - Interne Support- und Moderationsvorgänge
    3. **Personenbezogene Daten**
        - Namen, Kontaktdaten und weitere personenbezogene Angaben
        - IP-Adressen und zuordenbare Verbindungsprotokolle

Vertraulich

- Accountinformationen und Supportanfragen
- Personenbezogene Inhalte aus Bewerbungen und Beschwerden
- Sonstige personenbezogene Daten, die im Rahmen berechtigter Aufgaben verarbeitet werden

3. Geschäftsgeheimnisse im Sinne des Geschäftsgeheimnisgesetzes werden nur insoweit als solche behandelt, wie die gesetzlichen Voraussetzungen erfüllt sind.
4. Informationen Dritter werden ebenfalls geschützt, soweit Brandnetz zu deren vertraulicher Behandlung berechtigt oder verpflichtet ist.

§ 3 – Geheimhaltungspflichten

1. Das Teammitglied verpflichtet sich, vertrauliche Informationen mit angemessener Sorgfalt vor unberechtigter Kenntnisnahme, Nutzung, Veränderung und Weitergabe zu schützen.
2. Vertrauliche Informationen dürfen ausschließlich für die jeweils übertragenen Aufgaben verwendet werden.
3. Insbesondere ist es untersagt:
   - Vertrauliche Informationen unbefugt zu veröffentlichen oder weiterzugeben.
   - Zugangsdaten oder persönliche Accounts anderen Personen zur Verfügung zu stellen.
   - Interne Daten ohne Berechtigung zu privaten oder fremden Zwecken zu verwenden.
   - Nicht freigegebene Informationen auf öffentlich zugänglichen Plattformen zu veröffentlichen.
   - Sicherheitsmechanismen oder Zugriffsbeschränkungen ohne Genehmigung zu umgehen.
   - Vertrauliche Informationen ohne Berechtigung in externe Dienste oder KI-Anwendungen einzugeben.
4. Die Weitergabe an andere Teammitglieder ist zulässig, sofern diese zur Erfüllung ihrer Aufgaben berechtigt sind und die Informationen hierfür benötigen.
5. Gesetzliche Offenlegungsrechte sowie die Ausnahmen nach § 7 dieser Vereinbarung bleiben unberührt.

§ 4 – Datenschutz und personenbezogene Daten

Vertraulich

1. Das Teammitglied verpflichtet sich, personenbezogene Daten ausschließlich im Rahmen der erteilten Berechtigungen und Weisungen des jeweils Verantwortlichen zu verarbeiten, soweit keine gesetzliche Verpflichtung zur abweichenden Verarbeitung besteht.
2. Es sind die anwendbaren Datenschutzvorschriften, insbesondere die Datenschutz-Grundverordnung (DSGVO), einzuhalten.
3. Personenbezogene Daten dürfen insbesondere nicht:
    - Unbefugt eingesehen, exportiert oder vervielfältigt werden.
    - An unberechtigte Dritte weitergegeben werden.
    - Auf privaten Cloudspeichern oder sonstigen nicht freigegebenen Diensten gespeichert werden.
    - Für private Zwecke oder zur Erstellung eigener Datensammlungen verwendet werden.
    - Über die eingeräumten Berechtigungen hinaus verarbeitet werden.
4. Das Teammitglied hat die jeweils geltenden internen Datenschutz- und Sicherheitsanweisungen zu beachten.
5. Vermutete oder festgestellte Datenschutzverletzungen sind unverzüglich nach Kenntniserlangung an die von Brandnetz benannte zuständige Stelle zu melden.
6. Diese Vereinbarung ersetzt weder gesetzlich erforderliche Datenschutzinformationen noch gegebenenfalls notwendige gesonderte Datenschutz- oder Auftragsverarbeitungsvereinbarungen.

§ 5 – IT-Sicherheit und Zugangsdaten

1. Das Teammitglied ist verpflichtet, die ihm zur Verfügung gestellten Zugänge und Systeme angemessen zu schützen.
2. Dazu gehören insbesondere:
    - Verwendung sicherer, individueller Passwörter
    - Aktivierung der Mehrfaktor-Authentifizierung, soweit vorgesehen
    - Vertrauliche Behandlung von Zugangsdaten und Tokens
    - Nutzung ausschließlich freigegebener Zugriffswege
    - Einhaltung der rollenbezogenen Berechtigungen
    - Unverzügliche Meldung verlorener oder kompromittierter Zugangsdaten

Vertraulich

3. Zugang zu internen Systemen darf ausschließlich im Rahmen der erteilten Berechtigungen erfolgen.
4. Das Teammitglied darf weder eigenmächtig Berechtigungen erweitern noch anderen Personen unberechtigten Zugang ermöglichen.
5. Sicherheitsvorfälle sind unverzüglich an die zuständige Administration oder Projektleitung zu melden.

§ 6 – Dokumente, Kopien und Aufzeichnungen

1. Vertrauliche Dokumente, Screenshots, Protokolle, Datenbankauszüge und sonstige Aufzeichnungen dürfen nur angefertigt werden, soweit dies für die übertragenen Aufgaben erforderlich und gestattet ist.
2. Eine Speicherung außerhalb ausdrücklich freigegebener Systeme bedarf einer entsprechenden Berechtigung.
3. Zulässige, aufgabenbezogene Sicherungskopien und Dokumentationen bleiben erlaubt.
4. Gesetzlich zulässige Beweissicherungen, gesetzliche Aufbewahrungspflichten und die Wahrnehmung eigener Rechte bleiben unberührt.

§ 7 – Ausnahmen von der Geheimhaltung

Die Geheimhaltungspflicht gilt nicht für Informationen, die:

1. Bereits rechtmäßig öffentlich bekannt sind oder ohne Pflichtverletzung öffentlich bekannt werden.
2. Dem Teammitglied nachweislich bereits rechtmäßig und ohne Geheimhaltungspflicht bekannt waren.
3. Von einem dazu berechtigten Dritten rechtmäßig ohne Geheimhaltungspflicht übermittelt wurden.
4. Unabhängig von vertraulichen Informationen eigenständig entwickelt wurden.
5. Mit vorheriger Zustimmung des Berechtigten offengelegt werden dürfen.
6. Aufgrund zwingender gesetzlicher Vorschriften oder einer rechtmäßigen behördlichen oder gerichtlichen Anordnung offengelegt werden müssen.

Unberührt bleiben insbesondere gesetzlich geschützte Meldungen von Rechtsverstößen, zulässige Offenlegungen zur Aufdeckung rechtswidriger Handlungen, Rechte gegenüber Behörden sowie die Wahrnehmung und Durchsetzung eigener Rechte.

Vertraulich

Soweit rechtlich zulässig und zumutbar, soll Brandnetz vor einer verpflichtenden Offenlegung informiert werden. Eine solche Information ist nicht erforderlich, wenn gesetzliche Schutzvorschriften oder behördliche Anordnungen entgegenstehen.

§ 8 – Geistiges Eigentum und Nutzungsrechte

1. Bestehende Urheber-, Marken- und sonstige Schutzrechte verbleiben bei den jeweiligen Rechtsinhabern.
2. Die Überlassung vertraulicher Informationen führt für sich genommen nicht zur Übertragung von Urheberrechten oder zur Einräumung weitergehender Nutzungsrechte.
3. Die zur Erfüllung der übertragenen Aufgaben erforderliche Nutzung der bereitgestellten Informationen und Systeme bleibt gestattet.
4. Nutzungsrechte an neu entwickelten Plugins, Quellcodes, Designs, Texten, Grafiken, Dokumentationen und sonstigen Arbeitsergebnissen sind, soweit erforderlich, gesondert zu vereinbaren.
5. Rechte an bereits bestehenden oder unabhängig entwickelten eigenen Werken des Teammitglieds bleiben unberührt.

§ 9 – Ende der Zusammenarbeit und Rückgabe

1. Mit Beendigung der Zusammenarbeit oder auf berechtigte Aufforderung von Brandnetz hat das Teammitglied die ihm überlassenen vertraulichen Unterlagen, Datenträger und sonstigen Materialien zurückzugeben.
2. Nicht mehr benötigte Kopien vertraulicher Informationen sind entsprechend den rechtmäßigen Anweisungen zu löschen.
3. Das Teammitglied hat die Nutzung von Brandnetz-Zugängen mit Entzug der entsprechenden Berechtigung einzustellen.
4. Gesetzliche Aufbewahrungspflichten sowie rechtlich zulässige Aufbewahrungen zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen bleiben unberührt.
5. Soweit eine sofortige Löschung aus technisch unveränderlichen Sicherungskopien nicht möglich ist, bleiben die betreffenden Informationen bis zur regulären Löschung geschützt und dürfen nicht erneut produktiv verwendet werden, sofern keine rechtmäßige Grundlage dafür besteht.

§ 10 – Dauer der Geheimhaltung

Vertraulich

1. Diese Vereinbarung tritt mit der Unterzeichnung durch beide Parteien in Kraft.
2. Die Geheimhaltungspflichten gelten während der Zusammenarbeit und für einen Zeitraum von drei Jahren nach deren Beendigung fort.
3. Für Informationen, die gesetzlich geschützte Geschäftsgeheimnisse darstellen, bestehen die Pflichten so lange fort, wie die Informationen die gesetzlichen Voraussetzungen eines Geschäftsgeheimnisses erfüllen und deren Schutz rechtmäßig verlangt werden kann.
4. Die gesetzlichen Pflichten zum Schutz personenbezogener Daten bleiben unabhängig von der vorstehenden Frist bestehen, soweit sie im jeweiligen Fall anwendbar sind.

§ 11 – Pflichtverletzungen und Haftung

1. Bei einer schuldhaften Verletzung dieser Vereinbarung richten sich etwaige Ansprüche nach den gesetzlichen Vorschriften.
2. Brandnetz kann bei Vorliegen der gesetzlichen Voraussetzungen insbesondere Unterlassung, Beseitigung oder Schadensersatz verlangen.
3. Die Haftung des Teammitglieds richtet sich nach den jeweils anwendbaren gesetzlichen Bestimmungen. Gesetzliche Haftungsbeschränkungen, insbesondere bei Vorliegen eines Arbeitsverhältnisses, bleiben unberührt.
4. Eine pauschale Vertragsstrafe wird durch diese Vereinbarung nicht begründet.
5. Die Geltendmachung von Ansprüchen setzt die jeweiligen gesetzlichen Voraussetzungen voraus. Eine automatische persönliche Haftung für sämtliche Schäden oder für Handlungen anderer Teammitglieder wird nicht vereinbart.

§ 12 – Verhältnis zu anderen Vereinbarungen

1. Diese Vereinbarung ergänzt gegebenenfalls bestehende Team-, Beschäftigungs-, Entwicklungs- oder Dienstleistungsvereinbarungen.
2. Sie begründet weder ein Wettbewerbsverbot noch ein allgemeines Abwerbeverbot.
3. Gesetzliche Rechte zur beruflichen Betätigung und zur Aufnahme anderer Tätigkeiten bleiben unberührt.
4. Eine Verpflichtung zur unentgeltlichen Tätigkeit oder ein Anspruch auf Vergütung wird durch diese Vereinbarung nicht begründet.

§ 13 – Anwendbares Recht

Vertraulich

1. Für diese Vereinbarung gilt deutsches Recht, soweit nicht zwingende gesetzliche Bestimmungen entgegenstehen.
2. Die gerichtliche Zuständigkeit richtet sich nach den gesetzlichen Vorschriften.
3. Zwingende Zuständigkeitsregelungen, insbesondere für etwaige arbeitsrechtliche Streitigkeiten, bleiben unberührt.

§ 14 – Änderungen und Teilunwirksamkeit

1. Änderungen und Ergänzungen dieser Vereinbarung sollen aus Nachweisgründen in Textform dokumentiert werden, soweit gesetzlich keine strengere Form vorgeschrieben ist.
2. Individuelle Vereinbarungen haben im gesetzlich vorgesehenen Umfang Vorrang.
3. Sollten einzelne Bestimmungen unwirksam sein oder werden, richtet sich die Rechtsfolge nach den gesetzlichen Vorschriften. Die Wirksamkeit der übrigen Bestimmungen bleibt bestehen, soweit gesetzlich zulässig.

§ 15 – Bestätigung und Unterzeichnung

Mit ihrer Unterschrift bestätigen beide Parteien den Abschluss dieser Vereinbarung.

Das Teammitglied bestätigt insbesondere, die Geheimhaltungs-, Datenschutz- und Sicherheitsverpflichtungen zur Kenntnis genommen zu haben.

Diese Vereinbarung wird beiden Parteien in einer dauerhaft zugänglichen Fassung zur Verfügung gestellt.

Vertraulich

Unterschriften

Ort, Datum (Dario Nüssler)	Ort, Datum (Pascal Röse)
Dario Nüssler Straße der Völkerfreundschaft 7 17192 Klink (Brandnetz)	Pascal Röse Am Exerzierplatz 13 21073 Hamburg (Brandnetz)

Teammitglied

Ort, Datum (Teammitglied)

(Teammitglied)

Vertraulich