This document sets out the policies and guidelines applied by Certria in its relationship with Customer, in particular to clarify the manner in which the Services and Equipment may be used by Customer and what manner of use is considered unacceptable by Certria. Certria's general terms and conditions (the "General Conditions"), Certria's service specification (the "Service Specification"), and Certria's Support and Service Level Schedule ("Support and Service Level Schedule"), are also part of the Agreement and apply to the Services and any Equipment provided by Certria.

CHAPTER A
INTRODUCTION

1. DEFINITIONS

In addition to the definitions set out in the General Conditions, the Support and Service Level Schedule and the Services Specification, the following definitions shall apply:

Authentication Details
mean the logins, user identities, passwords, security questions, keys, tokens, URLs and other details that may be used to access the Service.

Blacklist
means a so called blacklist or block list which is a basic access control system that denies entry or access to a specific list or range of users or network addresses or IP addresses, as a result of which email sent by a user or from a network address or from an IP address that is on the blacklist will not reach its intended destination or recipient.

DDoS
means Distributed-Denial-of-Service.

DoS
means Denial-of-Service.

DRDoS
means Distributed-Reflected-Denial-of-Service.

Infrastructure
means the Equipment, Service and Instances that support the flow and processing of information, including storage, servers and networking components.

ICANN
means Internet Corporation for Assigned Names and Numbers, a not-for-profit public-benefit corporation, which is among other responsible for managing the Internet Protocol address spaces and assignment of address blocks to regional Internet registries, for maintaining registries of Internet protocol identifiers, and for the management of the top-level domain name space.

IRC
means Internet relay chat.

Mail Bomb
means
- *(i)* e-mailing copies of a single message to many receivers; and/or
- *(ii)* sending large or multiple files or messages to a single receiver with malicious intent.

RIPE
means Réseaux IP Européens, i.e. a collaborative forum open to all parties interested in wide area Internet Protocol networks and the (technical) development of the Internet.

SIDN
means the foundation, incorporated under the laws of the Netherlands, for Internet Domain Registration in the Netherlands (Stichting Internet Domeinregistratie Nederland)

Spam
means unsolicited bulk messages.

Malicious Software
means any type or form of malicious or hostile Software, including but not limited to computer viruses, worms, trojan horses, and spyware.

World Wide Web
means a system of interlinked documents that runs over the Internet.

2. GENERAL

2.1. **Certria aims to** promote a high level of responsible behavior in connection with the use of its Services, as well as, amongst others, the use of the Internet and the use of email. For this purpose, Certria has created the Certria Policies.

2.2. **All Customers must** comply with the Certria Policies and Customer is required to ensure that its End Users are aware of and comply with the Certria Policies, as though such End User were a Customer. A breach of the Certria Policies by an End User will also be considered a breach of the Certria Policies by Customer.

3. CONTACT PERSONS

3.1. **Customer shall** designate

(i) contact persons whom Certria may contact at any time in connection with (suspected) violations by Customer or its End Users of the Certria Policies,

(ii) contact persons whom Certria may contact at any time in the event of an Emergency.

3.2. **Customer shall provide** to Certria a means of contacting said contact person(s) at any and all times, and Customer shall ensure that the information set out in the Customer Portal with respect these contact persons is and remains up to date.

4. AUTHENTICATION DETAILS

4.1. **Some Services may** only be accessible through the use of Authentication Details. Customer is solely responsible for the maintenance, security and use of its Authentication Details. All consequences and losses relating to the use of Customer's Authentication Details, whether or not Customer has authorized that use, shall be for Customer's sole account, including all business and communication conducted with Certria through the use of its Authentication Details.

4.2. **To the extent possible**, Customer shall change its Authentication Details immediately upon receipt thereof by Customer, and Customer shall change the Authentication Details regularly thereafter. Customer will ensure that it will employ best practices when generating Authentication Details.

4.3. **If Customer knows** or suspects that the security of its Authentication Details has been compromised, or that its Authentication Details are misused, Customer must, as soon as possible, notify Certria and immediately change its Authentication Details.

CHAPTER B
ACCEPTABLE USE POLICY

5. USE OF SERVICES

5.1. **Customers shall** – and shall ensure that its End Users – only use the Services for lawful purposes and shall refrain from any use that breaches the Agreement or any applicable law.

5.2. **Without prejudice to the law** that applies to the Agreement, the Customer acknowledges and agrees that the

Customer's use – and its End User's use – of the Services is to be compliant with (mandatory) law of Bulgaria, as well as with other laws applicable to Customers or its use of the Service.

5.3. **Customer shall** refrain from any use of the Services which may have an adverse effect on Certria's good name or standing, or may cause damage to Certria's business operations, or may subject Certria to litigation.

5.4. **Specific activities** that are prohibited include, but are not limited to:

(i) terrorism;
(ii) threatening harm to persons or property or otherwise harassing behavior;
(iii) compromising the security (or tampering with) system resources or accounts of other Customers or of any other Internet sites or intranet sites without the proper authorisation;
(iv) violating local export control laws for Software or technical information;
(v) the use or transmission or distribution of any data or material protected by Intellectual Property Rights without proper authorisation;
(vi) the manufacture or use or distribution of counterfeit, pirated or illegal software or other product;
(vii) providing or offering compensation to End Users based on download volume, unless Customer knows – or has no reason to doubt – that such End Users are using Customer's services only for lawful purposes and for the distribution or dissemination of their own data or material, or of data or materials for which they have the proper authorisation to distribute or disseminate the same;
(viii) fraudulently representing products or services;
(ix) Spamming, phishing, DoS attacks, DDoS attacks, DRDoS attacks without proper authorisation;
(x) defamation, zoophilia, child pornography, and child erotica;
(xi) intentionally accessing a computer system or Infrastructure structure component without authorization or exceeding authorized access levels thereof;
(xii) activities that may result in the placement or inclusion on a Blacklist of Customer, Customer's IP address(es) and/or IP address(es) assigned by Certria to Customer; and
(xiii) facilitating, aiding, or encouraging any of the foregoing activities.

5.5. **Customer acknowledges that** any use by Customer and/or its End Users of the Services in breach of the Acceptable Use Policy could subject Customer and/or its End Users to criminal and/or civil liability, in addition to other actions by Certria outlined in Chapter G of the Certria Policies and in the General Conditions.

6. ELECTRONIC MESSAGES / ANTI-SPAM

6.1. **Customer may not**

(i) send electronic messages that in any way is or may be in breach of applicable law;
(ii) send or propagate Spam and shall not allow its End Users or third parties to send or propagate Spam via Customer's IP addresses;
(iii) send, propagate, or reply to Mail Bombs and shall not allow its End Users or third parties to send or propagate Mail Bombs via Customer's IP addresses; or
(iv) alter the headers of electronic messages to conceal Customer's address or to prevent receivers from responding to messages.

6.2. **Customer shall** refrain from any activities that may result in the placement of Customer or Customer's IP address(es) on a Blacklist. Certria reserves the right to charge Customer three hundred Euros (€ 300. --) per hour in consulting fees for any remedial actions that Certria elects to take in the event that, as a result of Customer's activities, Certria's servers or IP address(es) are placed in any third-party filtering software or Blacklist.

6.3. **Bulk messages** are only permitted if

(i) the Customer has obtained the explicit consent from each of the recipients via double opt-in, and/or
(ii) applicable law permits the sending of such messages without the recipients' consent. Customer is obliged to offer in each electronic message, an easily accessible functioning unsubscribe mechanism, and Customer shall immediately cease sending electronic messages to a recipient after the recipient has unsubscribed.

7. INTERNET USE

7.1. **Customer is prohibited from** posting or transmitting unlawful material on or via the Internet or the World Wide Web.

7.2. **Certria is entitled to** actively block ports or IP addresses for the Network, in the event that such is – in Certria's reasonable view – necessary to preserve or protect the security and performance of the Network or the Internet or the World Wide Web. An overview of the blocked ports or IP addresses may be requested in writing by Customer from Certria.

7.3. **Without prejudice to the generality of Clause 7.2.** of the Acceptable Use Policy, Certria shall in any event actively block the following ports for its Network:

(i) UDP/137 – Netbios;
(ii) UDP/139 – Netbios;
(iii) TCP/135 till 139 – Netbios; and
(iv) TCP/445 – Smb.

7.4. **If Certria reasonably suspects** that Customer is subject to a DoS attack, DDoS attack, DRDoS attack or another attack and (in Certria's reasonable opinion) such attack negatively affects the Infrastructure, Certria shall be entitled to immediately block access to Customer's Infrastructure. In the event that Customer is subject to repetitive attacks, and Customer does not successfully take measures to prevent that future attacks may negatively affect Certria's Infrastructure, then Certria shall be entitled to immediately terminate the Agreement by sending a written notice to Customer.

8. IRC USE

8.1. **Customer is prohibited from** posting or transmitting inappropriate material via the use of IRC or to otherwise use IRC in a manner that is in breach of the Acceptable Use Policy. For the purpose of this clause, prohibited use of IRC include so called 'eggdrops' and 'psybnc shell hosting'.

8.2. **Without the prior written consent** of Certria, which Certria may grant or deny in its sole and absolute discretion, Customer is prohibited from hosting an IRC server, regardless whether it concerns a stand-alone IRC server or an IRC server that connects to global IRC networks.

9. USE OF THE CUSTOMER PORTAL

9.1. **Subject to** the terms of use applied from time to time by Certria EOOD, and subject to the provisions of the Agreement, and Customer's compliance therewith, Certria shall arrange that Certria EOOD will grant a non-exclusive, non-transferable, non-assignable, non-sublicensable and royalty free right to use the Customer Portal during the Term. Use of the Customer Portal by or on behalf of Customer shall be at Customer's risk andresponsibility.

9.2. **Customer shall** observe each and any instruction of Certria EOOD regarding the use of the Customer Portal.

10. USE AND REGISTRATION OF *(INTERNET)* DOMAINS/IP ADDRESSES/AS NUMBERS

10.1. **Customer shall comply** with the policies, guidelines, terms and conditions applied from time to time by the organisation or entity which is responsible for the management (registration and/or distribution and/or giving into use) of an (Internet) domain, such as – for example – ICANN and SIDN.

10.2. **Customer shall comply** with the policies, guidelines, terms and conditions applied from time to time by the organization or entity which is responsible for the management (registration and/or distribution and/or giving into use) of IP addresses and AS numbers, i.e. the regional Internet registries of RIPE.

11. RESTRICTIONS ON USE OF SHARED WEB HOSTING SERVICES

11.1. **Customer may not:**

(i) use the Shared Web Hosting Services in a manner that may interfere with or otherwise disrupt services to other customers of Certria or Certria's infrastructure or that may cause an Emergency;
(ii) knowingly allow any other website or hosting server to link to content stored on Certria's systems. At least 75% of any content stored on Certria's systems must have associated HTML, PHP or similar files at the Shared Web Hosting Service linking to the content stored on the Shared Web Hosting Services;
(iii) exceed the Shared Web Hosting Services limits, such as allotted diskspace or bandwidth;
(iv) run scheduled tasks, such as cron entries, with intervals of less than fifteen (15) minutes;
(v) run stand-alone, unattached server side processes or deamons on the Shared Web Hosting Platform;

(vi) send more than 50 emails per minute/500 emails per hour; and/or
(vii) use Shared Web Hosting Services for hosting Mailer Pro, Push button mail scripts, proxy scripts/anonymizers, autoSurf/PTC/PTS/PPC sites, spiders, crawlers, indexers, banner-ad services (commercial banner ad rotation).

11.2. **If Certria detects** failed login attempts to the Shared Web Hosting Service, it may, without notice and without obligations of any kind, ban network access from the source of those failedattempts.

CHAPTER C
ABUSE COMPLIANCE POLICY

12. ABUSE HANDLING REQUIREMENTS

12.1. **In connection with** use of Certria Services, Customer shall adopt and apply an abuse handling procedure which is compliant with the Certria Policies, with the law that applies to the Agreement and with any other law applicable to Customer.

12.2. **Customer shall log** *(date and timestamp)* each Abuse Notification (as defined below) received by Customer from Certria and from third parties, including the nature of the notification (e.g. copyright infringement), as well as Customer's response to such complaint, and the moment that Customer deems the Abuse Notification to be resolved.

12.3. **Customer shall maintain** the log in respect of each Abuse Notification for a minimum of two (2) years after the date that Customer deems such Abuse Notification to be resolved. Customer will provide Certria with a copy of its Abuse Notification log, upon Certria's request.

12.4. **Customer shall ensure** the availability of sufficient and properly trained personnel to ensure that Customer's End Users comply with the Certria Policies and to apply Customer's abuse handling procedure and to handle the volume of abuse notifications that arrive without backlogs.

13. ABUSE PROCEDURE

13.1. **If Certria is notified** by a third party (including any law enforcement authority) of a (suspected) violation by Customer and/or the End-User of the Acceptable Use Policy and/or any applicable law (an "**Abuse Notification**"), Certria shall notify Customer hereof by way of email or such other method of communication as Certria deems appropriate.

13.2. **Customer shall**, within the response period or remedy period set forth in Certria's notification (the "**Remedy Period**"), take remedial action to cure the violation and within the Remedy Period inform Certria of the actions taken by Customer.

13.3. **In some cases**, Certria may grant the Customer the option to contest the alleged violation by filing a counter notice (a "**Counter Notice**"). If Customer chooses to file a Counter Notice, Customer must use the online form made available to Customer for this purpose. Certria shall review the submitted information and may (in Certria's sole discretion) decide to reject Customer's Counter Notice, and require Customer to take immediate remedial action, if – in Certria's sole discretion – Customer's or the End-User's content or actions are unmistakably unlawful and/or may subject Certria to third party claims and/or litigation.

13.4. **If Certria does not** reject Customer's Counter Notice, Customer shall - upon Certria's request - provide a deposit or a bank guarantee or a parent guarantee or other security satisfactory to Certria. The amount of the security will be determined by Certria at its sole discretion. The security is intended to cover Customer's obligations, and any claim of Certria, under the indemnity specified in the General Conditions. Furthermore, in the event that Customer files a Counter Notice, Customer shall within two (2) days of its response to Certria notify Certria whether an attorney will be representing Customer and, if so, which attorney.

13.5. **Customer shall provide** Certria with all documents and information in connection with the Abuse Notification without cost and on first demand.

13.6. **As a condition to** the *(continued)* provision of Services and/or to resuming the provision of Services, Certria shall be entitled to require Customer:
(i) to execute a cease and desist declaration; and/or - as appropriate -

(ii) to confirm in writing that Customer's End User who was responsible for the violation, has been permanently excluded from using the Service.

14. REPEAT INFRINGERS AND LIVE VIDEO STREAMS

14.1. **As part of** its abuse handling procedure, Customer should make reasonable efforts to detect repeated efforts by its End Users to store or transfer or distribute – on or via Customer's services –

(i) materials or data that violate or infringe the Acceptable Use Policies; or

(ii) that Customer previously deleted or disabled further to receipt of an AbuseNotification.

14.2. **Customer shall** immediately terminate the provision of service to an End User – and terminate an End User's access to the Service – in the event that such End User is discovered to be a repeat infringer or violator of the Certria Acceptable Use Policies.

14.3. **In the event** Customer's services are repeatedly used for streaming of live video and/or audio, Customer shall offer an online tool to trusted third parties (or their agents) to allow them to immediately terminate live video streams that are infringing on the intellectual property rights of these trusted third parties.

CHAPTER D

FAIR USE POLICY

15. IP CONNECTIVITY

15.1. **The IP Connectivity Service** is provided for Customer's consistent, fair, and reasonable use.

15.2. **Customer's use of** IP Connectivity shall be deemed unfair and unreasonable, if Certria determines (in its sole discretion) that Customer's actual or projected use of IP Connectivity exceeds, or is likely to exceed, the monthly Committed Bandwidth or Committed Data Traffic, and such use affects the provision of services by Certria to other Certria customers. If the Customer has not agreed to Committed Bandwidth or Committed Data Traffic, then for the purpose of interpreting this clause 15.2 only, the Committed Bandwidth or Committed Data Traffic (as applicable) shall be deemed the lowest value of the Committed Bandwidth or Committed Data Traffic offered by Certria for the respective Service.

15.3. **Customer's use of** IP Connectivity is deemed to be inconsistent, if Customer's use thereof results in irregular Bandwidth or Data Traffic usage patterns, either on a per server basis or as part of a group of Customer's servers/Instances.

16. CLOUD SERVICES

16.1. **Compute Capacity of** the Cloud Platform for the Public Cloud Services is provided to Customer on a shared basis. To protect the performance and integrity of the Cloud Platform, Customer shall, in respect of Public Cloud Service, ensure that its use of Compute Capacity shall be fair and reasonable.

16.2. **Customer's use of** Compute Capacity shall be deemed unfair and unreasonable by Certria, if Customer's use exceeds Certria's overbooking factor (as determined in the Service Specification) in such a way that (in Certria's reasonable opinion) it may affect the performance of other Infrastructure on the Cloud Platform.

16.3. **Storage components of** the Cloud Platform are provided to Customer on a shared storage system, and therefore Customer's use of the Cloud Services may affect the performance (such as latency, storage bandwidth and IOPS) of the storage system as a whole. To protect the performance and integrity of the Cloud Platform, Customer shall ensure that its use of the storage shall be fair and reasonable.

17. SHARED WEB HOSTING SERVICE

17.1. **Certria's Shared Web Hosting Platform** is made available to Customer on a shared basis. To protect the performance and integrity of the Certria Shared Web Hosting Platform, Customer shall ensure that its use of Shared Web Hosting Services shall be fair and reasonable.

17.2. **Customer's use** of the Shared Web Hosting Services shall be deemed unfair and unreasonable, if:

(i) Customer uses the Shared Web Hosting Services in such a way that (in Certria's reasonable opinion) it affects the performance of the Shared Web Hosting Platform or causes an Emergency;

(ii) the database size exceeds the total disk space allotted to Customer on the Shared Web Hosting Platform by 30%;
(iii) IMAP exceeds 5 connections per IP address;

(iv) twenty-five percent (25%) or more of the system resources are used in connection with Shared Web Hosting Services for longer than ninety (90) seconds at a time. Activities that could cause this excessive use include, but are not limited to, CGI scripts, FTP, PHP, HTTP; and/or
(v) Customer runs any MySQL queries longer than twenty (20) seconds. MySQL tables should be indexed appropriately.

CHAPTER E
SECURITY POLICY

18. INFRASTRUCTURE CONFIGURATION

18.1. **Certria promotes** a high level of responsible behavior in connection with the use of Certria services and requires that users of Certria Services do the same. For this reason, Certria has established information security requirements for all Certria Services, including standards for the basic configuration of Infrastructure, the use of Authentication Details and the use of effective Malicious Software detection and prevention.

18.2. **Customer is advised**

(i) to back-up (critical) data and system configurations on a regular basis and store such data in a safe place, and
(ii) not to connect its Infrastructure via a wireless connection,
(iii) to keep the Software operated or used on the Infrastructure up to date, and accordingly to install updates and patches on a regular basis without undue delay after becoming available,
(iv) to operate and/or use adequate measures against Malicious Software on theInfrastructure.

19. MONITORING / REPORTING

19.1. **Customer shall implement** logging and monitoring measures for security-relatedevents.

19.2. **Customer shall** immediately report to Certria's NOC any security-related event that may materially impact Certria's Infrastructure, Certria's organisation or Certria's provision of services to other customers. Customer shall make the log in relation to such event immediately available to Certria upon Certria's request, and shall follow any directions given by Certria's as may be required to contain or correct the event.

CHAPTER F
FACILITY OPERATIONS POLICY

20. INTRODUCTION

20.1. **The Facility Operations Policy** contains a code of conduct for the day to day operations – and the presence of Customers – at a Data Center.

20.2. **Certria has adopted** the Facility Operations Policy for the security and safety of Customers, Customer's employees, Customer's (sub)contractors and/or the Infrastructure.

21. SHIPMENTS

21.1. **Each Customer shall** observe the shipping and receiving policies adopted from time to time by Certria with respect to shipment of Equipment to and from the Data Center.

21.2. **Customer shall** notify Certria of any intended shipment to the Data Center, at least *two (2)* business days before the intended delivery date of the Equipment. Such notification will be given by Customer by means of the shipment notification form available in the Customer Portal. In relation to administrative activities performed by or on behalf of Certria in connection with such shipment, Certria shall be entitled to payment by Customer of a shipment charge in the amount of:

(i) fifty Euros (€ 50. --), in the event that Customer has timely notified Certria of the intended shipment; or

(ii) two hundred and fifty Euros (€ 250.--), in the event that Customer has not notified or has not timely notified Certria of the (intended) shipment.

21.3. **All costs related to** Customer's shipments of Equipment to or from a Data Center shall be at Customer's cost and expense.

21.4. **Customer is responsible for** cleaning up and disposal of all materials and equipment used for Customer's shipment. Customer shall ensure that such shipment material is removed from the Data Center on the same day as the date of delivery. If Customer does not comply with this provision, Certria shall charge a clean up fee to Customer.

21.5. **Certria is not responsible for** shipments to or from the Data Center. All shipments made or sent by Customer shall be at Customer's own risk.

22. PHYSICAL STORAGE

22.1. **Data Centers** have little or no storage area. Certria cannot assure the safety of Colocated Equipment that is not secured in the Housing Space or contained within the Data Center.

22.2. **If Customer is not** ready to install certain equipment, and it is too bulky to contain within the Housing Space, Certria may require Customer to store the Equipment in a storage area at Customer'sexpense.

23. CONDUCT AT DATA CENTER

23.1. **With the exception of** an Emergency, Customer with a 24/7 access card shall give Certria at least *one (1)* hours' notice for access to the Data Center and/or Housing Space, and Customer without a *24/7* access card shall give Certria at least *twenty-four (24)* hours' notice for access to the Data Center and/or Housing Space.

23.2. **Customer shall identify** itself at the reception of the Data Center by showing a valid ID (Driver's license, Passport, Country ID) and explain the purpose of its visit. Customer is required to sign in and out when entering and exiting the Data Center, whereby Customer shall indicate its time of entry and time of exit. The reception will hand over an access card. Customer shall at all times during the visit wear the access card which needs to be fully visible. Before leaving, Customer shall - at the reception – hand in the access card; failure to do so may result in a Service Charge.

23.3. **On a daily basis**, Customer may allow a maximum of three (3) persons to access the Data Center. A Service Charge shall be due by Customer for each person entering the Data Center, with the exception of a holder of a 24/7 access card or those persons who are accompanying such card holder access card. Only the first person will be charged. Access shall be charged on a thirty (30) minutes interval basis, with a minimum of one (1) hour.

23.4. **Customer shall provide** Certria with a list of persons authorized for access to the Housing Space and Colocated Equipment, which Customer may amend from time to time upon written notice to Certria. Customer shall be responsible for all persons who receive access on behalf of Customer.

23.5. **Certria may require**, at its sole discretion, that a Certria representative escorts any representative of Customer accessing the Data Center and/or Housing Space. Also, the house rules of the Data Center may provide that the owner or lessor of the Data Center may - under certain circumstances - require that one of its staff escorts any representative of Customer who are accessing the Data Center and/or Housing Space.

23.6. **If Certria personnel provides** an escort during Customer's access to the Data Center and/or Housing Space, such escort shall be considered an additional Service for which Certria shall charge Customer an additional Service Charge (escort charge) in addition to all escort charges imposed on Certria by the Data Center owner. If a representative of Customer is accompanied by an escort provided by the owner or lessor of the Data Center while accessing the Housing Space, Customer shall pay Certria all related escort charges that may be imposed on Certria.

23.7. **Customer shall**

(i) at all times, act in a professional manner,

(ii) not interfere in any way with Certria's use or operation of the Data Center or with the use or operation of any Equipment installed by other parties, including Equipment of other Customers. Should Customer require to (re)move or disconnect another party's Equipment to service its own

Equipment, Customer shall contact Certria and request Certria's instructions prior to any such movement, removal and/or disconnection, taking into account a 48 hour notice period,

(iii) refrain from operating any Equipment that may constitute a safety hazard,

(iv) not perform any tests that may cause harm or damage to – or interfere with – the Certria Network, the Housing Space and/or the Data Center, and

(v) ensure that it closes doors after use, in order to maintain a closed and secure environment and thus ensuring an efficient environment for the fire protection system and climate control system, and

(vi) lock the Rack before leaving. If in doubt, Customer shall consult the facility manager of the Data Center or – in the facility manager's absence – another employee of Certria.

23.8. **Certria may** at its sole discretion remove any of Customer's personnel or Customer's (sub)contractors or third party agents, if such person does not comply with any Certria Policy, or any instruction provided by an employee of Certria.

23.9. **In case of an Emergency**, such as a fire, which in general will be indicated by the sound (slow whoop) of an alarm system, Customer shall immediately evacuate the Data Center.

23.10. **Smoking is prohibited** in the entire Data Center. Eating and drinking is prohibited in the areas within the Data Center where the Housing Space and/or Equipment is located.

23.11. **Within the areas** where the Housing Space and/or Equipment is located, Customer shall refrain from any activity that may cause dust particles. One of the reasons for this prohibition is that dust particles may set off the automatic alarm system. If in doubt, Customer shall consult the facility manager of the Data Center or – in the facility manager's absence – another employee of Certria.

23.12. **Unless expressly required** under any (product) insurance warranty, Customer shall not bring any packaging material into the areas where the Housing Space and/or Equipment is located and any (card board) boxes shall be unwrapped by Customer in the loading bay area. Should Customer – in view of a (product) insurance warranty – require to bring packaging material into the areas where the Housing Space and/or Equipment is located, it will notify Certria thereof in advance. Certria will then assign a member of its staff to accompany Customer during Customer's presence in the areas where the Housing Space and/or Equipment is located. Customer is under an obligation to remove all packaging material from the areas where the Housing Space and/or Equipment is located, within *one (1)* hour after entering the relevant area.

23.13. **Customer shall** immediately report any irregularities and/or alarms, noticed by Customer during its presence in the Data Center, to the facility manager of the Data Center or – in the facility manager's absence – another employee of Certria.

24. EQUIPMENT REQUIREMENTS

24.1. **Unless expressly agreed** otherwise in writing by Certria, all Equipment shall be installed and maintained by or on behalf of Customer in accordance with the following criteria:

(i) Telecommunication lines shall be extended from an organized and protected distribution frame;

(ii) Spare parts for the Equipment shall be kept within the confines of the Housing Space;

(iii) AC and DC power distribution shall take place within the Housing Space, to the extent available;

(iv) Equipment density shall be consistent with floor loading at the Facility;

(v) All cables shall be tied and harnessed in an orderly fashion;

(vi) Equipment shall be in full compliance with telecommunications industry standards and in accordance with Certria's requirements and specifications; and

(vii) Equipment shall comply with applicable laws, rules and regulations in the jurisdiction where located (including specifically in Europe, but without limitation, the EU EMC Directive (89/336/EEC) and the EU Low Voltage Directive (73/23/EEC)), as amended from time to time.

24.2. **Customer is expressly prohibited** from installing any AC UPS Equipment in the Housing Space or at the Data Center in general.

24.3. **Customer must ensure that** Equipment with AC power supplies have a power factor of 0.85 or higher.

CHAPTER G

25. INVESTIGATION

25.1. **Certria reserves the right to** conduct an investigation, based on
- *(i)* suspected violations of the Certria Policies; and/or
- *(ii)* (potential) security risks to its Infrastructure; and/or
- *(iii)* a valid request of the relevant (law enforcement) authorities.

25.2. **As part of this investigation**, Certria may, acting reasonably
- *(i)* gather information from or about Customer;
- *(ii)* if relevant, gather information from a complaining party; and/or
- *(iii)* review and investigate Customer's security log referenced in Clause 19. Customer is obliged to fully cooperate with any such investigations by Certria.

26. CERTRIA ACTION

26.1. **To the extent legally required**, Certria is authorised to grant relevant law enforcement authorities access to Customer's content, information and/or Infrastructure, as well as any information gathered in the investigation conducted by Certria under clause 25.1.

26.2. **Upon request of a third party**, Certria shall be entitled to disclose identifying Customer information to said party in connection with a (suspected) breach of the Certria Acceptable Use Policies to the extent required by law (such to be determined in Certria's discretion).

26.3. **Certria shall be entitled** to take action, legal or otherwise, against Customer and/or and End User, in the event that the use of the Service by Customer or its End User(s), breaches the Certria Policies, or Customer fails to comply with any obligation under the Certria Policies. The appropriate action will be determined by Certria, in its sole discretion, and may include:
- *(a)* suspension or termination of any or all of the Services in accordance with the General Conditions;
- *(b)* (selective) IP or port blocking;
- *(c)* reinstallation of the Services;
- *(d)* imposing limits on the use of Service (such as imposing limits on the speed of the data the Customer may transmit and/or receive with the Service);
- *(e)* restarting the Service,
- *(f)* blocking access at the router and/or switch level of Customer's Infrastructure;
- *(g)* denying Customer (physical) access to Infrastructure;
- *(h)* providing binding instructions to Customer in regards of the use of the Services, and/or
- *(i)* placing files infected by Malicious Software in quarantine.

27. DISCLAIMER

27.1. **Without prejudice to the above** or any other provision of the Certria Policies, Certria does not intend to review, monitor or control as a precautionary measure content sent or received by Customers using the Services. Accordingly, Certria is not responsible or liable for the content of any communications that are transmitted by or made available to Customer or its End Users, regardless of whether they originated from the Network or the Services.

27.2. None of the provisions of this Chapter G or any of the other Chapters of the Certria Policies shall in any way limit or prejudice any other rights or remedies Certria may have.