Confirmation of domain name email address

The main authority for domain names is the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN have required that all registrars validate a domain registrant 's email address since 1st January 2014.

The email address of a registrant will be validated upon the purchase, transfer or modification of the registrant name within a domain name unless that email address has already been validated. Should any of these three things occur, you will be send an email requiring an affirmative response. Failing to provide a response within 15 days triggers automatic suspension of the domain name.

This new validation is required for all existing generic top level domains (.com, .net etc.). There is currently no validation needed for country code top level domains such as .co.uk which are not under the authority of ICANN.

The same validation process will take place if a WHOIS Data Reminder Policy (WDRP) notice, 30 day expiration notice or five day expiration notice bounces. It is therefore of paramount importance to ensure your domain's WHOIS data is correct.

You must not disclose your password to any of CyberHive's systems or services to any third party.

We reserve the right to take whatever measures we deem appropriate and proportionate to a breach of the AUP, up to and including suspending or terminating one or more of your CyberHive accounts. All cases are considered on an individual basis. Following suspension of your account, you must send a formal letter to CyberHive undertaking not to commit any future "abuse" before we consider reinstating the account.

CyberHive does not allow credits or refunds for any outages resulting from a suspension or deletion of an account under this Policy. You are still required to meet the terms laid out in your contract, including any minimum contract period.

Internet access

While connected to the Internet your system must meet applicable Internet Engineering Task Force standards. These can be found at ftp://ftp.ripe.net/mirrors/rfc/std/

You must not use your account to obtain unauthorised access to any computer or Service. You are responsible at all times for the use of your account – whether by you or by a third party. You must not send email or any other type of electronic message that has a forged address or which affects the performance or functionality of remote machines.

You may not use our services to perform port scanning or probing, except with the explicit permission of the operators of the remote machines or networks targeted.

Your machine or network must not be configured in such a way that others can exploit it to disrupt the Internet. This includes, but is not limited to, ensuring that your network cannot be exploited as an Open Mail Relay, an Open Proxy Server or a Smurf Amplifier.

You must ensure that your system is not used for the sending of unsolicited bulk email or any other form of "abuse" whether it originates on your system or is from a third party. If you are running a web server on your own system you are solely responsible for the security and setup of that server. You are also responsible for all traffic that passes through your server.

Usenet / Mailing Lists / Email

Unsolicited Commercial Email (UCE) is advertising material sent and received by email without the recipient either requesting such information or otherwise explicitly expressing an interest in the material advertised. CyberHive considers the sending of both commercial and non-commercial unsolicited bulk email to be unacceptable behaviour.

Any mailing lists run through CyberHive's network must adhere to the “confirmed opt-in” principle. To make it simple to join lists it is common to offer an option to join by means of a checkbox on the same web page that collected an email address for another purpose. This checkbox should require an explicit action to add the address to the mailing list rather than having joining as the default setting.
To prevent forged subscriptions, a confirmation of any request is required before adding the new email address. This is most easily achieved by sending an email to the requesting address and then making it a joining requirement that this special email is responded to. Further details on this can be found in the Best Current Practice document, available at:

https://www.linx.net/good/bcp/mailinglist-bcp-v1_0.html

You must not use CyberHive's service for any of the following purposes:

- Initiating or propagating 'chain' or pyramid emails
- Sending bulk or unsolicited emails
- Using your CyberHive account to receive responses from “abusive” mailing
- To email a person after they have specifically asked you not to mail them
- To subscribe a third party to a mailing list without their permission

You must not send email or post articles with headers modified to disguise their true source. It is your responsibility to ensure that a real email address is present and obvious to a human. It is unacceptable to arrange for replies to the email to be sent to another user or machine unless their explicit permission has been granted.

You must not attempt Denial of Service attacks or mail bombing. This includes, but is not limited to, sending an excessive number of emails to the same host and sending viruses attached to an email.

You must not post articles which contravene the charter of the newsgroup to which the posts are made. This includes posting binary attachments to “non-binary” newsgroups and sending unsolicited posts of a commercial nature to any group. The only exception to the binary rule is to always allow the use of cryptographic signatures, such as PGP.