

Incident Response and Security Policy

Despite everyone's best efforts and audits, security incidents are inevitably part of the business. Your security is important to us, and we are fully committed to its security and that of our clients. We continue to maintain a culture of transparency and truthfulness, which also extends to our approach to reporting security incidents. Ultra.cc will take the following actions:

Close all connections to Ultra.cc servers, WHMCS, or any other accessible place to resolve the incident rapidly. As soon as any Incidents reported or discovered by us, we will publish this on our communication channels at the earliest, including our website, our Twitter page, our subreddit, our community Discord server, and the Incident response page. We will also start emailing the clients affected, but it might take some time for all the emails to be dispatched.

In case you're experiencing issues with your services, please check the status page at status.usbx.me. It's most likely you will see some maintenance work related to your node. If there is no ongoing maintenance, feel free to open a support ticket to investigate your Issues and guide you accordingly.

Policies

To continue trusting us, we have published a few essential bits of highly important information for you. We want to be as transparent as possible and share all the information that we store and how we store and use them.

- Abuse Policy
- Cookies Policy and sub-processors
- Global privacy practices
- Password policy
- Username policy
- Privacy policy
- Refund policy
- Sensitive Data removal policy
- Username policy
- Terms of Service

Security first partners and vendors

- We assess third-party partners and vendors for fit and security risk based on the services they provide. We also make sure the right technical and contractual commitments are in place.
- We use N+1, Tier 3 data center vendors with your availability and security in mind—and with physical security.
- Use of VLAN, To keep the data safe and secure and to avoid possible sneaking, we use private VLANs at our network providers [Novoserve.com](https://www.novoserve.com) and [YISP.nl](https://www.yisp.nl).

How Can You Help

As we describe in our Terms of Service and on our security page, we do our utmost to ensure that Ultra.cc is safe and secure - to help us protect it further, you can help us in the following ways:

- Adhere to our password policy. You can read our password policy [here](#).
- Moderate your account sharing, do not share your account with people you do not know.
- Notify Ultra.cc if you notice any unauthorized use of or access our platform through your account, including any unauthorized use of your password.
- Enable two-factor authentication (2FA).

Report a security event, vulnerability, or abuse

- Please notify Ultra.cc support to report a security event, like unauthorized account usage or a suspected data breach.
- Remove sensitive data - Need sensitive data removed from Ultra.cc? See our [Ultra.cc Sensitive Data Removal Policy](#)
- Read our [Content Abuse Policy](#) and how you can report any copyright content abuse.

Revision #9

Created 13 November 2020 21:25:27

Updated 4 June 2023 10:24:26 by warp