XMedius

XMedius Cloud Solutions - Security Roles and Responsibilities

Purpose

The purpose of this document is to clearly establish the roles and responsibilities of XMedius, XMedius partners and customers in the security of the XMedius Cloud solutions. Since security is a joint responsibility between the above parties, having clear definitions allows each party to make sure they put the appropriate measures in place to ensure the overall continuity of security.

Customer role and responsibilities

- Keep up-to-date information about the account owner and billing contact.
    - The account owner has full authority over the account and has the right to request for administrators to be added or removed from the account.
    - The billing contact will receive all billing formation, including CDR, invoice, non-payment information, low credit balance
- Ensure that the administrator's accounts are given to people that should have the authority to exercise that role which includes:
    1. Requesting fax numbers and number porting
    2. Managing users, including provisioning and deprovisioning
    3. Managing (other) administrators, including provisioning and deprovisioning
    4. Managing security configurations
    5. Having access to account data, including fax data
    6. Having access to usages and billing information
    7. Managing any other account configuration under the administrator's control
- Ensure that user accounts are given to people that have the right to use the service as part of the customer business function
- Ensure that users are aware of the service usage restrictions as mentioned in Section 4 of the Term & Conditions (https://portal.xmedius.com/terms_of_service)
- Make sure that all administrators and users protect their account credentials appropriately
- Configure the appropriate password policies and/or properly configure SSO integration
- Select the appropriate retention policies for fax and SafeBoxes
- Configure, in the account, the customer email server addresses (or enable SPF check) to prevent fraudulent impersonification of customer users (faxing by email)
- Configure any other security/administrative features or setting under the control of the account's administrators
- Ensure that the use of the service is in compliance with the customer's applicable regulations, including but not limited to (HIPAA, HDS, GDPR)

- Communicate to XMedius any special/sectorial regulation applicable to the use of the service.
- Ensure the service usage is not abusive to the point it affects to overall stability and availability of the service (Ex: making excessive API calls)
- Ensure that no penetration test or any other intrusive security testing is performed by the customer without the express consent of the XMedius Security Team
- Provide XMedius advance notice of significant changes in traffic usage in order for XMedius to properly manage the service capacity
- Report to XMedius any fraudulent use of the service or suspicious activities as soon as they are discovered
- In some instances, the customer may give to their reseller/partner, from which they bought the service, the right to manage their account (giving them **FULL** administrative capability in the account). In such instance, it is the responsibility of the customer to ensure that the reseller/partner is meeting all the customer security requirements. XMedius is not responsible for the partner/reseller actions on the customer account.
- In some instances, the reseller/partner from which they bought the solution has **FULL** administrative rights in their account. In such instance, it is the responsibility of the customer to ensure that the reseller/partner is meeting all the customer security requirements. XMedius is not responsible for the partner/reseller actions on the customer account.

XMedius role and responsibilities

- Manage and secure the service infrastructure, including
    - Network segregation
    - System hardening
    - Software update and patching
    - Business continuity & disaster recovery process
    - Incident response process
    - Backups
    - Capacity management
    - Access control to the infrastructure and customer data
    - Monitoring
    - IDS/FIM/Anti-Virus/Anti-Malware/Vulnerability scanners
    - Penetration and segmentation testing
- Manage the provisioning/deprovisioning of customer accounts (when XMedius is doing the provisioning)
- Provide support to customers in the configuration and usage of the service
- Manage all telecom aspects regarding the service including provisioning and deprovisioning
- Notify customers of issues with the service (via the helpdesk Maintenance and Status board (https://support.xmedius.com/hc/en-us/sections/200642646-Status-Maintenance)

- Notify customers of any security breach that may have resulted in the disclosure of their data.
- Maintain a formal ISMS and ISO 27001 certification

See XMedius Cloud Services privacy policy for more details on XMedius engagements and security controls to protect customer data https://www.xmedius.com/en/privacy-policy/

Reseller/Partner role & responsibilities

If applicable,

- Manage the provisioning/deprovisioning of customer accounts
- Provide support to customers in the configuration and usage of the service
- Obtain written approval from the customer to manage their account (i.e. the "AUTHORIZATION AND CONSENT FORM REGARDING CLIENT ACCOUNT ACCESS" form)
- Report to XMedius any fraudulent use of the service or suspicious activity as soon as they are discovered