BUSINESS VOICE & SECURITY

The security features every business voice system should have and the information and assurances you should always be looking for.

1

ENCRYPTION

Your solution should be 'top level' military grade. This means using AES 256-bit encryption (which means 'advanced encryption standard') and ensures you are encoding data that is simply unbreakable, no matter where your employees are based or however they're accessing the internet.

2

AUTHENTICATION

How is your workforce authenticating? Only authorised individuals should be able to access your business voice solution using two-factor authentication (2FA) such as biometrics (face ID, fingerprint) text, authenticator app.

3

BACK-UP & RECOVERY

Can data and service be restored quickly and efficiently with minimal data loss or disruption? Your service should mitigate for in-case-of-emergency (ICE) scenarios and outages, ensuring you can continue to stay in contact with customers, operate systems and access business-critical data.

4

INFRASTRUCTURE & ENVIRONMENT

You should be partnering with a vendor whose infrastructure is protected and regularly assessed. It's good to see evidence of details on their data security pledge, understand the physical security of their infrastructure as well as how they process data.

5

EMPLOYEE TRAINING

93% of all company breaches are caused by an employee. Part of your voice system training should focus on ensuring the best security behaviours are adopted and that your workforce understands the modern threat landscape.

6

COMPLIANCE & STANDARDS

Do you adhere to the relevant regulations and standards? Many procurement decisions are reliant on them. You may not have heard of the FISMA audit or the NIST SP 800-53 R5 accreditation, but they are used to foster best practice, ongoing cyber improvement and crucially allow organisations to use a common security language.

Visit our website to find out more about our Business Voice portfolio

8x8 vaioni