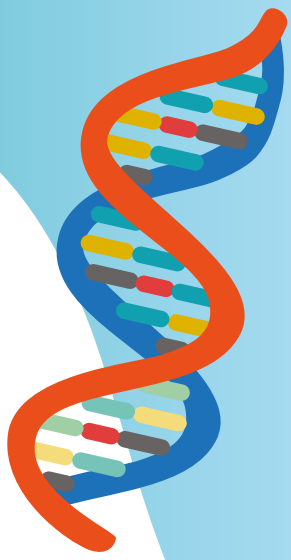
ICE
TRUSTED IT PARTNER

ICE's Ultimate Guide to

IMPLEMENTING A SECURE, SCALABLE, IT INFRASTRUCTURE

ICE
TRUSTED IT PARTNER



As an IT provider with 25 years of experience working in biotech, we created this guide to help companies establish a proper IT foundation. The solutions outlined are based on suggested and identified processes that are crucial in establishing a base IT infrastructure. The driving factor behind this design is to create a secure, reliable, and redundant network that is highly flexible and easy to scale.

THE IDEAL IT FOUNDATION

Solutions, procedures, and policies every biotech company should have in place

CENTRALIZED IDENTITY ACCESS MANAGEMENT SOLUTION

IP and data are frequently a startup's most important assets in this sector. Given how many businesses deal with sensitive data daily, security hygiene is crucial for both individuals and businesses. Consolidating data via a centralized identity management system is the first and most crucial step in dependable security hygiene for enterprises.

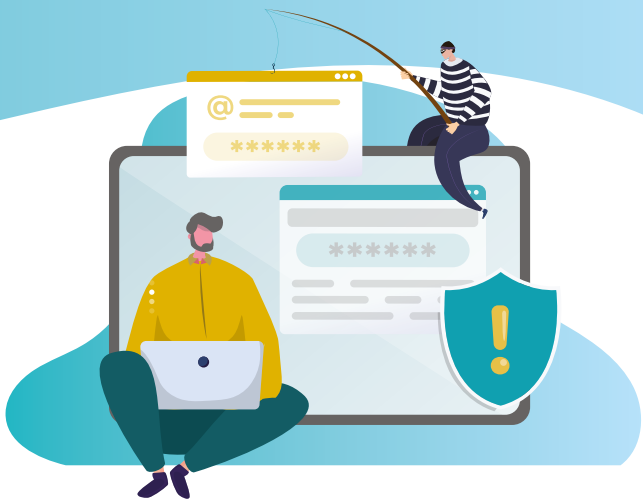
Other benefits include:

A seamless user experience: Using one set of credentials reduces hassle, removes the need to remember numerous login/password combinations, and reduces the need for password resets.

Consistency: Maintain data accuracy and consistency across all platforms. Automatically record and audit user and access activities.

Automated provisioning and deprovisioning: Faster provisioning of new users with fewer human mistakes. Deprovisioning eliminates a user at once from all platforms, eradicating zombie accounts and shielding users from dangers from malicious actors.

Streamlined threat mitigation: With better visibility, breaches are easier to detect and isolate.



SINGLE SIGN-ON (SSO)

Cybercriminals' main goals are usernames and passwords. Hackers have a chance every time a user connects to a new program. Because users only log in once a day and use a single set of credentials, SSO decreases the attack surfaces.

Enterprise security is increased by limiting the login to a single set of credentials. When workers are required to use unique passwords for every program, they typically don't. 59% of people use the same or similar passwords across many accounts. A hacker is therefore likely to be able to access other company systems if they get access through one inadequately protected website.

When SSO is a component of your IAM system, it makes use of a central directory to regulate user access more finely to resources. This makes it possible for businesses to adhere to laws that demand giving users the right authorization.

MULTI-FACTOR AUTHENTIFICATION (MFA)

MFA is the quickest, easiest way to verify that users are who they claim to be. Instead of relying just on an email address and a password, it operates by requesting confirmation from users for several other factors. Authentication factors include things like your password, your device, or a security key. They can also include things like your own fingerprint (biometrics), your location, or the amount of access you have depending on adaptive rules.

PASSWORD POLICIES

By implementing a strong password policy, your business can make it more difficult for cybercriminals to gain access to its confidential data.

Cybercriminals often use brute force attacks to guess passwords, and if they’re able to crack your password, they may be able to gain access to sensitive information. If they manage to gain access to this information, they may put you out of business before you even get started.

MOBILE DEVICE MANAGEMENT (MDM)

MDM enables IT to automate, regulate, and safeguard administrative rules on laptops, cell phones, tablets, and other devices linked to a company's network.

Employees are growing accustomed to utilizing the software, hardware, and operating system of their choosing. IT departments have a distinct set of difficulties while distributing and integrating corporate information and resources because of the variety of mobile devices.

To control end-user devices, mobile device management often uses a combination of corporate policies and certificates, on-device settings, applications, backend software, and hardware. The goal of mobile device management is to maximize device support, organizational functionality, and security while allowing a degree of user flexibility, such as the use of BYOD.

ENDPOINT BACKUP

All your devices will be protected against data loss by an endpoint backup system that is designed for businesses. Every endpoint will be backed up using Endpoint Backup to allow for swift data recovery. These systems automatically gather and store every version of every file on all your PCs to prevent data loss. These options can be set up to execute backups periodically throughout the day or to back up files continuously. Accuracy checks are performed on files to prevent corruption or loss.

NEXT-GENERATION ENDPOINT DETECTION & RESPONSE (EDR)

Centralized endpoint security is essential for shielding the machine and data of your users from harmful activities. Modern artificial intelligence (AI), machine learning, and tighter integration of network and device security are used in next-generation endpoint security to offer more comprehensive and adaptable protection than conventional endpoint security systems.

Next-generation endpoint protection incorporates real-time analysis of user and system behavior to analyze executables—allowing users to detect fileless “zero day” threats and core advanced technologies prior to and during execution, and take immediate action to block, contain, and roll back those threats. In addition to addressing threats, next-generation tools also proactively learn from threats and continuously adapt methods to combat them with greater speed and efficiency.

Enterprises of all sizes are being targeted by the next generation of cyberattacks. Utilizing next-generation endpoint security can better arm your organization’s defenses against modern threats and the evolution of attack campaigns.

ENDPOINT ENCRYPTION

This will protect systems from unauthorized physical access to data on the drives of these devices. Encryption is the process of encoding or scrambling data so that it is unreadable and unusable unless a user has the correct decryption key. Endpoint encryption protects the operating system from the installation of "Evil Maid" attacks that can install a keylogger or corrupt boot files and lock files stored on laptops, servers, tablets, and other endpoints to prevent unauthorized users from accessing the data.

Volumes of important data are shared and stored by employees at companies on network drives, browsers, email, USB sticks, cloud storage services, and other media, all of which are prone to security breaches. Sensitive information including financial information, client names and addresses, and private company plans may be included in this data. The data is far more protected against theft when it is encrypted.

SECURE FILE SHARING (GROUPS, PERMISSIONS, SHARES)

By using encryption, authentication, and access control to make sure that only authorized users can access the data, secure file sharing offers a mechanism to safeguard sensitive data. Data that has been encrypted is transformed into unintelligible code that can only be decoded by authorized users using the encryption key. Access control restricts who may access files and authentication verifies that users are who they say they are.

Maintaining privacy and adhering to data protection laws need secure file exchange. Strict rules regarding the management of sensitive information are in place in various areas, including healthcare and biotechnology. Heavy penalties and other legal repercussions may follow noncompliance with these rules.

Cyberattacks are growing more frequent and sophisticated in the digital age, so organizations and people must take precautions to safeguard sensitive data from them. Unsecure file sharing puts private data at risk from online threats including malware, phishing, and ransomware.

Employees must be able to access data from any place, on any device, in the fast-paced corporate climate of today. Users may safely access data from any device, including laptops, tablets, and cellphones, thanks to secure file sharing. As a result, employees are more productive and efficient since they can work whenever and from wherever.

EMAIL SECURITY

Email security is integral to protecting companies from external threats but is also essential to protecting a brand's customers from outbound threats. Without sufficient email security strategies, companies open themselves, their clients, and their customers to the consequences of cyber security incidents such as phishing, data breaches, and business email compromise (BEC).

For any firm, ignoring email as a security concern is a risky oversight. According to professional services network Deloitte, 91 percent of all cyberattacks started with phishing emails in 2020.

There are several dangers associated with insufficient email security, including phishing, takeover, data theft, and social engineering assaults. Users' passwords and accounts that could include private and important consumer information are vulnerable to phishing attempts. Employees who reuse passwords for several platforms in both their personal and professional lives run the danger of credential theft, which might make a company less secure if any of these accounts are hacked or made public because of a data breach.

VPN REMOTE ACCESS

While VPN technology isn't new, Remote Access VPN as a service is a modern network security solution for everyday business needs. Your teams need to work safely from anywhere, anytime, and on any device. A Remote Access VPN creates an encrypted tunnel between your organization's resources, endpoint devices on the network, and the employees using them — shielding all online activity from outside users and safeguarding sensitive areas of the network.

If you have remote workforces or are working from remote locations, a secure connection to your company network is vital. A remote-access Virtual Private Network tunnel encrypts online traffic, allowing you to access resources and keep data safe while working across any Wi-Fi connection.

Remote access to work files is essential in today's climate. A remote office VPN enables you to securely access resources and applications on your company network whilst keeping them away from unauthorized users and hidden from public view.