Empowering remote work with advanced IT solutions

microsourcing

Contents

An overview of MicroSourcing's remote work IT setup plan

In today's dynamic work environment, the ability to operate effectively from any location is crucial. Our remote work IT setup plan is designed to create a seamless, secure and efficient working environment for our employees from the comfort of their homes.

This plan outlines the necessary hardware, software and support structures that will be provided to ensure that all team members can perform their duties without any technological issues.

Key components of this plan include standardized IT hardware, robust internet security protocols, centralized endpoint management and comprehensive IT support.

We aim to replicate our office environment's functionality and security in a remote setting, providing all employees with the necessary tools and resources to be productive, connected and secure.

MicroSourcing's work-from-home IT infrastructure's five key pillars

Consistency and reliability

Ensuring all remote employees have access to a standardized set of tools and technology, including desktops with the latest operating system, uninterrupted power supplies and essential software. This consistency is key to minimizing compatibility issues and streamlining remote operations. Below is an overview of our five key pillars:

Security and compliance

As an ISO 27001 certified organization, maintaining the highest level of data security and compliance is non-negotiable. Our remote IT infrastructure will adhere to these standards, implementing robust security measures like endpoint security with Checkpoint Harmony and web and application filtering to protect sensitive company and client data.

User responsibility and independence

Recognizing the importance of individual responsibility, particularly in a remote setting, the plan emphasizes the role of employees in managing their internet connectivity and maintaining a conducive work environment.

Centralized control and management

Utilizing centralized management tools like Active Directory and ManageEngine Desktop Central, we aim to maintain control and visibility over all IT assets, ensuring efficient management and rapid response to any IT issues.

Efficient support and resolution

Establishing a comprehensive IT support system, including remote assistance for software or technical issues and clear protocols for hardware issues. The use of a ticketing tool for IT support ensures a streamlined, trackable process for resolving any IT-related queries or problems.

Continuous improvement and adaptation

Regularly reviewing and updating the IT infrastructure to keep pace with the evolving technology landscape and the changing needs of our remote workforce.

Standard IT hardware provisions

To ensure optimal performance and reliability for our remote workforce, we provide a standard set of hardware. This package includes:

1. **Standard desktop:** each remote employee will be provided with a high-quality desktop computer equipped with Windows 11 Pro. This operating system is chosen for its advanced features, user-friendly interface and robust security measures.
2. **Uninterruptible power supply (UPS):** alongside the desktop, each setup will include a UPS unit. The UPS is critical in providing power backup in the event of power outages or fluctuations within the home environment. This not only protects the hardware from potential damage due to power issues but also ensures that work is not interrupted, maintaining productivity and safeguarding data integrity.

Why is a standardized setup important?

Three reasons: consistency, ease-of-support and customizable flexibility. While we emphasize the importance of a standardized IT setup for our remote operations offering, our approach is also characterized by a significant degree of flexibility to accommodate the unique requirements of our clients. This dual approach ensures both consistency and customizability, offering several key benefits:

- **A uniform user experience:** a standard setup with a common hardware and software baseline ensures a consistent and reliable user experience for all employees. This uniformity is essential for efficient training, collaboration and communication.
- **Streamlined IT support:** standardized equipment simplifies IT support. Familiarity with a common set of tools and configurations allows our IT team to diagnose and resolve issues swiftly and effectively.
- **Efficient tech management:** managing IT assets becomes more streamlined with standardization, facilitating easier updates, maintenance and security management.
- **Adaptability to client needs:** recognizing that different clients may have unique requirements, we offer the flexibility to customize both hardware and software configurations. This includes providing different types of hardware, specific software suites or unique network setups as per the client's specifications.
- **Tailored solutions:** our capability to adapt and provide customized solutions ensures that we can meet the diverse needs of our clients. Whether it's specific performance requirements, unique software applications or particular security protocols, we are equipped to tailor our IT solutions accordingly.
- **Enhanced client satisfaction:** this flexibility underscores our commitment to client satisfaction. By offering customized solutions, we can cater to specific business needs, leading to improved productivity and efficiency for our clients.

By offering a foundational standard IT setup along with the flexibility to customize based on client needs, we position ourselves as a versatile and client-centric organization. This approach allows us to maintain high standards of consistency and efficiency while also being adaptable to the evolving and diverse needs of our clients.

Internet connectivity: a user responsibility

In our remote work setup offering, each individual must have a reliable and stable internet connection. To this end, we have established a policy where the end-users – our remote employees – are responsible for securing and maintaining their own internet connections. This approach ensures that each team member can choose an internet service provider (ISP) that best fits their location, budget and specific needs.

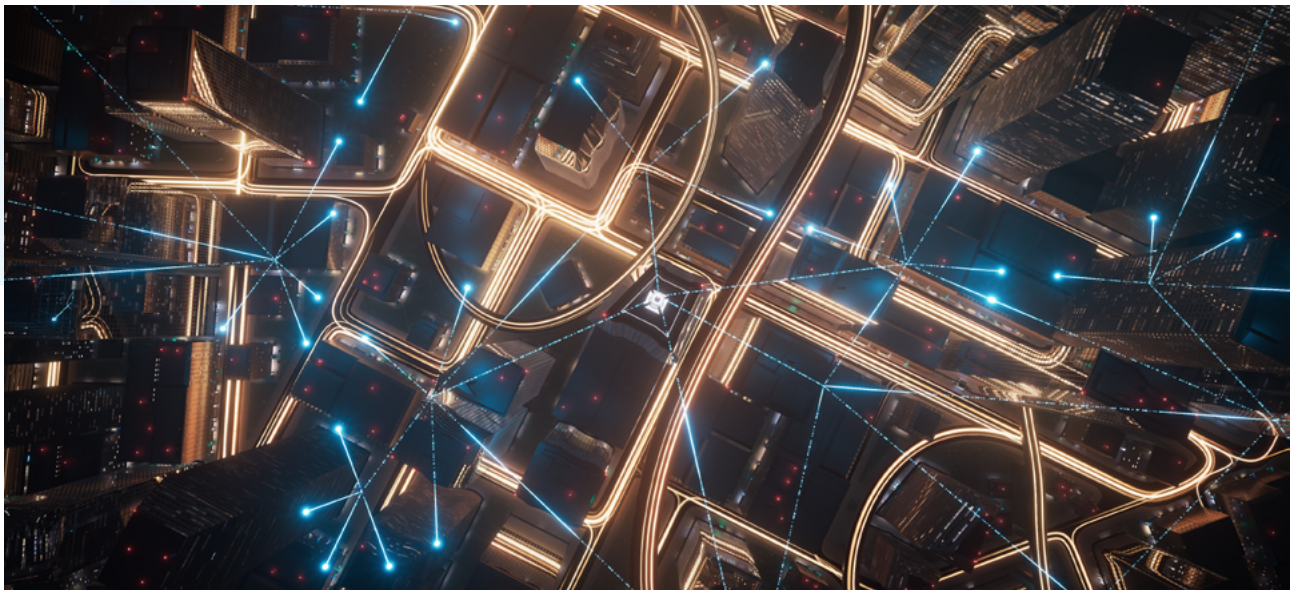
Key aspects of this policy include:

1. **Personalized connectivity:** employees have the flexibility to select an ISP based on their personal preferences and regional availability, allowing them to optimize for speed, reliability and cost.
2. **Empowering employees:** this responsibility empowers our employees to manage a key aspect of their remote work environment, ensuring they are invested in maintaining a stable connection.
3. **Independence and accountability:** by making internet connectivity a personal responsibility, employees develop a sense of independence and accountability, crucial traits for effective remote working.

Minimum requirements for internet connections

To ensure a smooth and efficient remote working experience, we recommend the following minimum requirements for internet connectivity:

- **Minimum speed:** a stable internet connection with a minimum download speed of 50 Mbps and a minimum upload speed of 25 Mbps. This speed is generally sufficient for most work-related tasks, including video conferencing, cloud-based applications and data transfers. In the case of clients who require higher speeds, we recommend employees upgrade their bandwidth to match the client's requirements.
- **Reliability:** we advise choosing an ISP known for its reliability and consistent service. Frequent disconnections or service interruptions can significantly hamper productivity and communication.
- **Latency:** a lower latency (ping) is preferable, especially for tasks that require real-time collaboration. The latency of different applications will depend on the location of the servers. Most cloud-based applications have CDNs which provide locally distributed traffic for better performance.
- **Data caps:** opt for plans with higher data caps or unlimited data usage. This is particularly important for roles that involve extensive online activities, large file transfers or a continuous online presence.
- **Backup plans:** where possible, having a backup internet solution, like a mobile hotspot, can be beneficial in case of primary connection failures.



Internet service providers in the Philippines and their infrastructure

In the Philippines, there are several reputable ISPs known for their robust infrastructure and high-quality internet services. These providers have made significant investments in their networks to ensure high-speed, reliable internet connectivity, which is crucial for remote work environments. Some of the notable ISPs include:

1. **PLDT:** one of the largest and most established ISPs in the Philippines, PLDT offers a range of fiber-optic internet plans that are ideal for heavy internet usage and large file transfers.
2. **Globe Telecom:** known for its extensive coverage and reliable service, Globe Telecom offers various internet plans that cater to different needs, including fiber-optic options.
3. **Converge ICT:** specializing in fiber internet, Converge ICT is recognized for providing high-speed internet services, particularly in urban areas.
4. **Sky Broadband:** offering a mix of fiber and cable internet services, Sky Broadband is another option for those seeking reliable internet connections with various plan choices.
5. **Eastern Communications:** known for its customer-centric approach, Eastern Communications provides both fiber and DSL internet services, focusing on reliability and personalized service.

There are also multiple small players available in the market based on the geographic location which can be selected by the employees.

These recommendations are designed to provide a guideline for our employees to ensure their home internet setup meets the basic requirements for an effective and uninterrupted remote working experience. However, we understand that internet availability and quality can vary greatly depending on the geographical location and encourage our employees to approach us for any assistance or advice in selecting the right internet plan for their needs.

Seamless network integration

In our remote work infrastructure, the integration of a centralized active directory (AD) controller plays a pivotal role. This system is designed to streamline the network management of all remote workstations and devices, ensuring seamless integration regardless of the geographical location of our employees.

Key elements of this setup include:

- **Remote access to centralized AD:** each employee's workstation is configured to connect remotely to our centralized AD. This connection is established through secure, encrypted channels to ensure both safety and efficiency.
- **Unified login credentials:** users will have a single set of login credentials managed by the AD, enabling access to all necessary work resources, including email, internal systems and applications. This unified approach simplifies access management for remote workers.
- **Automated policy enforcement:** the AD controller allows us to automatically enforce security policies and access controls across all remote endpoints. This includes password policies, access rights and other user permissions.
- **Synchronization and updates:** regular synchronization with the central AD ensures that all user and system updates are consistently applied across the network, maintaining uniformity and compliance.

The benefits of centralized user management and network security

The integration of a centralized AD for our remote workforce offers numerous benefits:

- **Enhanced security:** centralized user management allows for stricter and more consistent security protocols. By managing all user credentials and access rights from a single point, we can quickly respond to security incidents and enforce company-wide security standards.
- **Improved efficiency:** with centralized management, administrative tasks such as adding new users, assigning roles or updating permissions become more streamlined and less time-consuming.
- **Consistency in user experience:** centralized AD ensures that all employees, regardless of their location, have uniform access to resources and a standardized approach to software and system updates.
- **Scalability and flexibility:** a centralized system can easily be scaled to accommodate more users and more complex organizational structures.
- **Reduced IT complexity:** by centralizing network management, IT teams can more effectively monitor, troubleshoot and maintain the network.
- **Compliance and audit-readiness:** a centralized system enables easier audit trails and reporting, as user activities and system changes are all recorded in a single, centralized location.

The implementation of a centralized AD is a cornerstone of our remote IT strategy, ensuring a secure, efficient and scalable network environment for all employees, regardless of their physical location.

Endpoint management with ManageEngine Desktop Central

In our remote work setup, managing and securing endpoints is a critical aspect. To address this, we utilize ManageEngine Desktop Central, a comprehensive endpoint management solution. This tool enables us to efficiently manage, control and secure all the endpoints in our network, including desktops, laptops and mobile devices, irrespective of their location.

Why do we use ManageEngine Desktop Central for our endpoint management?

1. **Centralized management:** provides a single console for managing all endpoints, greatly simplifying the tasks of IT administrators.
2. **Automated patch deployment:** ensures that all endpoints are up to date with the latest software patches, reducing vulnerabilities.
3. **Software deployment:** facilitates the remote installation, updating and removal of software applications across endpoints.
4. **Asset management:** keeps track of hardware and software assets, providing detailed inventory reports for effective resource management.
5. **Remote control:** offers the capability to remotely troubleshoot issues on any endpoint, minimizing downtime and enhancing support efficiency.
6. **Configuration management:** allows for the remote configuration of system settings, ensuring compliance with organizational policies.
7. **Enhanced security:** by automating patch management and ensuring that all endpoints adhere to security policies, the system significantly reduces the risk of security breaches.
8. **Increased productivity:** the remote troubleshooting and assistance capabilities ensure that any issues employees face are resolved quickly, leading to minimal disruption and maintaining high productivity levels.
9. **Scalability:** the tool is highly scalable and capable of managing a few to several thousand endpoints, making it suitable for businesses of all sizes.
10. **Compliance management:** helps in maintaining compliance with various regulatory standards by ensuring that all endpoints are consistently managed and monitored.
11. **Customizable alerts and reports:** offers customizable alerts and comprehensive reports, providing insights into the health and performance of the IT infrastructure.

ManageEngine Desktop Central is a vital component in our IT infrastructure, offering a streamlined, efficient and secure approach to managing the diverse and distributed endpoints of our remote workforce.

Robust endpoint security with Checkpoint Harmony

Checkpoint Harmony is an integral part of our endpoint security strategy, offering a comprehensive suite of security features tailored to protect our remote work environment. We utilize various features of Checkpoint Harmony to ensure a multi-layered defense against a wide range of cyber threats, including ransomware.

The key features we employ include:

- **Endpoint compliance:** ensures that all endpoints meet our organization's security standards and compliance requirements. This feature checks for the presence of necessary security software, OS updates and system configurations.
- **URL filtering:** provides control over web access by blocking malicious or unauthorized websites, thereby preventing web-based threats, and enforcing web usage policies.
- **Media encryption and control:** secures sensitive data on removable storage devices, such as USBs, and controls their usage on company endpoints. This prevents data leakage and loss through external media. By default, we disable USB mass storage using our group policy settings.
- **Threat emulation:** utilizes advanced sandboxing techniques to inspect suspicious files and URLs in a safe environment, protecting against zero-day threats and unknown malware.
- **Anti-malware:** offers robust protection against malware, spyware and other malicious software, using real-time scanning and heuristic analysis to detect and neutralize threats.
- **Full disk encryption:** integration with ManageEngine and Windows Bitlocker ensures the encryption of the entire hard drive of the endpoint, ensuring that data remains secure and inaccessible in the event of theft or loss.
- **Forensics:** provides detailed forensic analysis capabilities, enabling the IT security team to investigate and understand the nature and impact of any security incident.
- **Threat extraction:** removes potentially dangerous elements from documents and files, delivering clean, safe content to the user and mitigating the risk of malware infections.
- **Behavioral guard:** employs behavior-based detection to identify and block advanced attacks that may bypass traditional security measures, offering an additional layer of protection.
- **Firewall:** integrates a firewall component to monitor and control incoming and outgoing network traffic, establishing a barrier against network-based threats.

By integrating these advanced features of Checkpoint Harmony into our endpoint security strategy, we ensure a resilient and adaptive security posture, crucial for protecting our remote workforce and maintaining the integrity of our IT infrastructure.

Secured internet access

As a service provider, we recognize the diverse needs of our clients and the importance of tailoring internet security measures to fit their unique business requirements. Using Checkpoint Harmony Endpoint, we offer customized web and application filtering solutions, ensuring both robust security and alignment with each client's specific operational needs.

Key aspects of our customized approach include:

- **Client-specific filtering policies:** we work closely with clients to understand their business operations and requirements, enabling us to create tailored web filtering policies. This includes blocking or allowing specific categories and sub-categories based on the client's business nature and preferences.
- **Flexible application control:** understanding that different clients may use a variety of applications, we offer customizable control settings. This allows clients to restrict or permit applications based on their business relevance and security considerations.
- **Adherence to default block lists:** while customization is key, we maintain a default block list for universally recognized harmful categories such as adult content, terrorism, tobacco, gambling, and social media (if approved by the client) to ensure a baseline level of security and compliance across all client setups.
- **Real-time adaptation to client needs:** our web and application filtering capabilities are not static. They are designed to evolve and adapt in real-time to changing client needs, emerging threats and evolving internet landscapes.
- **Engagement in approval processes:** we involve clients in the approval process for filtering policies, ensuring transparency and alignment with their policies and values.

Why a controlled internet access environment is crucial?

Controlled internet access is particularly important in a client-focused environment for several reasons:

- **Targeted security:** customizing internet access based on client-specific needs ensures that security measures are both effective and relevant, offering protection against threats pertinent to their industry or operational context.
- **Data protection compliance:** different clients may be subject to varying regulatory requirements, especially concerning data protection. Tailored web and application filtering help in complying with these specific regulations.
- **Enhanced productivity:** by aligning internet usage policies with the client’s business operations, unnecessary distractions are minimized, thereby boosting productivity.
- **Network resource optimization:** custom filtering aids in efficient bandwidth utilization, ensuring that critical business applications receive the necessary resources.
- **Risk mitigation:** tailored access controls are crucial in mitigating risks, including insider threats and accidental data exposure, by ensuring that only relevant and safe web content and applications are accessible.

By offering a customizable approach to web and application filtering via Checkpoint Harmony Endpoint, we not only uphold stringent security standards but also cater to the unique requirements and preferences of each client, enhancing both their security posture and operational efficiency.

Reliable patch management: ManageEngine Endpoint Central

Effective patch management is a critical component of our IT infrastructure, particularly in a remote work setting. We employ ManageEngine Endpoint Central to streamline and automate the patch management process. This approach ensures that all systems are up to date with the latest security patches, bug fixes and performance improvements.

The key steps in our patch management process using ManageEngine Endpoint Central include:

1. **Patch discovery:** automatically identifies the need for patches across various software and operating systems in our network.
2. **Patch testing:** before deployment, patches are tested in a controlled environment to ensure compatibility and prevent potential issues.
3. **Automated deployment:** patches are automatically deployed to endpoints, reducing the need for manual intervention and ensuring timely updates.
4. **Scheduling and rollout:** patches are scheduled and rolled out in a manner that minimizes disruption to end-users, often during off-peak hours.
5. **Compliance reporting:** post-deployment, the system generates reports confirming the successful application of patches and compliance with organizational policies.
6. **Vulnerability assessment:** regularly assesses the network for vulnerabilities that patches can address, ensuring ongoing protection against known issues.

The practice of regular updates and patch management is essential to us for several reasons:

- **Security enhancement:** regular patching is one of the most effective ways to protect against cyber threats. Patches often include fixes for security vulnerabilities that, if left unaddressed, could be exploited by hackers.
- **Bug fixes:** patches correct known bugs in software, resolving issues that could cause system crashes or data loss, thereby enhancing overall system stability.
- **Performance improvements:** many updates include optimizations that improve the efficiency and speed of software and systems, contributing to better user experience and productivity.
- **Compliance with standards:** regular patching ensures compliance with various security standards and regulations, which often mandate up-to-date security practices.
- **Mitigation of exploit risk:** by patching systems promptly, the window of opportunity for attackers to exploit a known vulnerability is significantly reduced.
- **Maintaining software integrity:** updates ensure that software functionalities are preserved and improved over time, aligning with evolving technology and user needs.
- **End-user protection:** regular updates also protect the end-users from potential security risks, ensuring their data and work remain safe.

By leveraging ManageEngine Endpoint Central for our patch management, we ensure that our remote workforce's systems are secure, stable, and optimized, mitigating risks and enhancing overall operational efficiency.

Comprehensive IT support

Our approach to IT support is geared towards providing comprehensive and efficient assistance for our clients' application and technical issues, emphasizing the importance of remote support in today's digital workplace.

Here's how we handle IT support:

The key steps in our patch management process using ManageEngine Endpoint Central include:

- **Ticketing tool:** we employ a specialized ticketing tool developed in-house to track and manage IT support requests from end users. This tool allows for efficient logging, tracking and resolution of issues, ensuring that no request is overlooked.
- **Service level agreements (SLAs):** SLAs are established for each type of ticket and subtype, based on industry standards. These SLAs define the expected time frame for response and resolution, ensuring that our support services are timely and consistent.
- **Automated ticket escalation:** to maintain service quality and adherence to SLAs, our system has predefined auto-escalation protocols for tickets. This ensures that any ticket requiring urgent attention is escalated to the appropriate level of support without delay.
- **Remote support focus:** our IT support is primarily remote, encompassing both technical assistance and hardware support. This remote-first approach enables us to provide prompt and effective support regardless of the client's location.
- **Communication and updates:** updates regarding the status and resolution of tickets are communicated to users via email. This keeps users informed about the progress of their requests and any necessary actions or information required from their side.

Our commitment to providing timely IT support is reflected in the following ways:

1. **SLA targets:** our IT department has set an ambitious SLA target to resolve 98% of tickets within the stipulated time frame each month.
2. **Tracking and reporting:** SLAs are closely monitored, with performance tracked both weekly and monthly.
3. **Accessibility:** our IT support team is accessible 24/7, with provisions for urgent support needs outside of these hours. Clients can raise tickets through multiple channels, ensuring ease of access.
4. **Response times:** the response times vary depending on the severity and type of the issue, in alignment with our SLAs. Urgent issues are prioritized to ensure minimal impact on the client's operations.
5. **Continuous improvement:** we regularly review and update our IT support processes and SLAs based on client feedback and evolving industry standards, ensuring that our support services remain relevant and effective.

Through our structured and client-centric IT support system, we ensure that all technical and application-related issues are addressed promptly and effectively, maintaining high standards of service and client satisfaction.

Hardware issue resolution

Our approach to hardware issue resolution is designed to be efficient and user-friendly, ensuring minimal downtime for our end users and client operations. The procedure is as follows:

1. **Initial reporting:** end users are required to report any hardware issues through our ticketing tool or designated support channels. This initial report should include a detailed description of the issue and any troubleshooting steps already taken.
2. **Remote diagnosis:** upon receiving a hardware issue report, our IT support team will first attempt to diagnose and resolve the issue remotely. This may involve guiding the user through certain steps or remotely accessing the system, if necessary.
3. **Determination of hardware fault:** if the IT team identifies a hardware fault that cannot be resolved remotely, the user will be instructed to prepare the equipment for return.
4. **Arrangement for equipment delivery:** users are requested to make arrangements to deliver the faulty equipment to our nearest office location. Users can themselves physically bring the equipment or instructions and assistance for packaging and shipping the hardware will be provided to ensure safe transit.
5. **Immediate replacement or repair:** we maintain a sufficient inventory of our standard hardware offerings on-site to facilitate immediate replacement or repair. Upon receiving the faulty equipment, it will be promptly replaced or sent for repair, depending on the nature of the issue.
6. **Return of equipment:** once the replacement or repair is complete, the equipment will be returned to the user, with all necessary steps taken to ensure that it is fully operational and meets our quality standards.

For end users, the following steps are recommended to ensure efficient resolution of hardware issues:

- **Accurate issue reporting:** provide a clear and detailed description of the problem in the initial report, including any error messages and troubleshooting steps already attempted.
- **Follow remote troubleshooting guidance:** cooperate with the IT support team during remote diagnosis and adhere to their instructions for troubleshooting.
- **Prepare equipment for return:** if a hardware fault is identified, follow the guidelines provided for safely packaging and shipping the faulty equipment or physical carrying of equipment.
- **Stay informed:** keep track of updates regarding the status of your hardware repair or replacement, which may be communicated via email or the ticketing system.
- **Provide feedback:** after the resolution of the issue, users are encouraged to provide feedback on the support process. This helps in continually improving our hardware support services.

By following these procedures and steps, we ensure that hardware issues are resolved swiftly and efficiently, minimizing disruption and maintaining high levels of productivity and user satisfaction.

Commitment to security: ISO 27001 certified since 2014

As a company, we are firmly committed to maintaining the highest standards of information security, which is demonstrated by our adherence to ISO 27001 standards. ISO 27001 is an internationally recognized standard that provides a framework for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS).

Key aspects of our adherence to ISO 27001 include:

- **Risk management:** we conduct regular assessments to identify and mitigate risks to our information security.
- **Data protection policies:** our policies and procedures are designed to protect data from unauthorized access, disclosure, loss and damage.
- **Employee training:** all employees undergo regular training on information security and are well-versed in our ISO 27001 compliant procedures.
- **Regular audits:** we conduct internal audits to ensure ongoing compliance with ISO 27001 standards and take corrective actions when necessary.
- **Continuous improvement:** our ISMS is subject to continuous improvement, adapting to new threats and changes in the information security landscape.

ISO 27001 certification has a significant impact on data security and client trust in several ways:

- **Enhanced data security:** the certification ensures that we have robust systems in place to protect data. This includes secure data handling processes, encrypted communications and secure network configurations.
- **Reduced risk of data breaches:** adhering to ISO 27001 standards significantly reduces the risk of security breaches and data leaks, protecting both our company and our clients from the potentially devastating consequences of such events.
- **Legal and regulatory compliance:** ISO 27001 aligns with many legal and regulatory requirements, reducing the risk of non-compliance penalties and legal issues related to data security.

Our ISO 27001 certification is more than just a badge; it is an integral part of our commitment to ensuring the highest level of security and trust in our relationships with clients.

Employee monitoring with ProHance

As part of our comprehensive IT services, we also offer an optional employee monitoring tool: ProHance. ProHance is a state-of-the-art monitoring solution designed to enhance productivity, efficiency and management oversight in remote work environments. This tool provides insights into work patterns and productivity, helping clients, managers and employees optimize their work processes.

Key features of ProHance include:

- **Activity tracking:** tracks employee activity during work hours, providing data on application usage, website visits and active or idle time.
- **Productivity analysis:** offers analytics on productivity patterns, helping to identify areas where efficiency can be improved.
- **Project and task management add-on:** enables managers to allocate tasks effectively and track project progress in real-time.
- **Time management add-on:** assists employees in managing their time more efficiently, with insights into time spent on various tasks and projects.
- **Customizable reports:** provides customizable reports for detailed insights, facilitating informed decision-making and strategy planning.
- **Data privacy compliance:** designed with a strong focus on privacy, ProHance ensures compliance with data protection regulations, respecting client and employee privacy and confidentiality.

The benefits of implementing ProHance

1. **Enhanced productivity:** by providing detailed insights into work patterns, ProHance helps in identifying and addressing productivity bottlenecks.
2. **Better resource nanagement:** helps our clients and their managers to understand how resources are being utilized, enabling more effective resource allocation.
3. **Improved project oversight:** facilitates better project management through real-time monitoring of project progress and task completion. This is an add-on module.
4. **Data-driven decisions:** the analytics and reports generated by ProHance support data-driven decision-making, enhancing overall operational efficiency.
5. **Balancing workload:** helps in balancing workloads among team members, leading to a more equitable and efficient work environment.
6. **Employee self-management:** empowers employees to self-monitor and manage their productivity, fostering a culture of self-improvement and accountability.

The implementation of ProHance is optional and can be tailored based on client preferences and policies. We ensure transparency in its use and seek consent from employees, prioritizing ethical considerations in monitoring practices. Clients have the flexibility to customize the settings of ProHance to align with their specific monitoring needs and ethical guidelines.

By offering ProHance as an optional tool, we provide our clients with an advanced solution to enhance workforce management and productivity, while upholding our commitment to ethical practices and employee privacy.

Frequently asked questions: MicroSourcing's work from home IT setup

Question: What standard hardware is provided for remote work setups?

Answer: We provide standardized hardware which includes a desktop computer equipped with Windows 11 and a UPS unit to ensure reliability and consistency across all remote setups. Configuration of the standard desktop hardware keeps on changing based on new technologies and upgrades in the industry. Your business development or the account manager will provide you with the details before the deployment.

Question: How does the company ensure internet connectivity for remote employees?

Answer: While employees are responsible for their own internet connectivity, we provide minimum recommended specifications to ensure a stable and efficient remote working experience.

Question: What security measures are in place for remote workers?

Answer: Our security measures include comprehensive endpoint management using Manage Engine Desktop Central, robust endpoint security with Checkpoint Harmony and adherence to ISO 27001 standards to protect against various cyber threats.

Question: How does the company handle patch management for remote systems?

Answer: Patch management is efficiently handled through ManageEngine Endpoint Central, ensuring that all systems are regularly updated with the latest security patches and software updates.

Question: What is the procedure for resolving hardware issues in remote setups?

Answer: If a hardware issue is identified, employees are required to deliver the faulty equipment for immediate replacement or repair. We maintain an inventory of standard hardware to facilitate this process.

Question: How does the company manage IT support for remote employees?

Answer: IT support is managed through a ticketing tool, with predefined Service Level Agreements (SLAs) for different types of issues. Our IT team provides remote technical support and updates on tickets are communicated via email.

Question: What are the company's SLA targets for IT support?

Answer: Our IT department aims to meet an SLA target of resolving 98% of tickets within the specified timeframe each month, with SLAs tracked weekly and monthly.

Question: What customization options are available for web and application filtering?

Answer: We customize web and application filtering based on client-specific business needs while maintaining a default block list for critical categories like adult content, terrorism etc.

Question: How does the company ensure compliance with ISO 27001 standards?

Answer: Compliance with ISO 27001 is ensured through regular risk assessments, data protection policies, employee training, internal audits and a commitment to continuous improvement in our Information Security Management System (ISMS).

Question: Are there any guidelines for employees to ensure efficient use of the IT support system?

Answer: Yes, employees are encouraged to provide clear and detailed descriptions of issues when raising tickets, follow instructions for remote troubleshooting, and provide feedback post-resolution to help us continuously improve our IT support services.

For more information, please visit our website or contact us today:

U.K./Europe: +44 20 3695 2586
U.S./Canada: +1 888-731-0023
Australia: +61 3 7003 9283

www.microsourcing.com

microsourcing