

# Your Data, Our Care.

*Infinit-O Information Security Compliance*

The optimum significance of securing  
and assuring the privacy of your data



we build  
great teams

**Infinet-O shares 15 years of experience in navigating data privacy laws and regulations. We guarantee strict compliance from the best information security practices with up to date ISO certifications.**

Continuously delight SMBs across the world, we support domain experts in Healthcare, Finance & Accounting, Research & Data, and Customer Support. We've been handling and managing an array of information for different industries, allowing us to fully understand the importance of data security. With this, we are proud and happy to share our comprehensive, heightened and robust information security and data privacy procedures in our drive for a more secured connectivity and cloud services usage.

## **Your Data**

We understand that simple firewall and antivirus software as your company's sole security measure may not be enough in this digital age. With the advancement of technology, data risks have also evolved rapidly, increasing security threats and cyberattacks. But at Infinet-O, we not only value your business but acknowledge the importance of information security especially in this digital age. For us, your peace of mind is as important as your business's success.

Fundamentally, companies are now more technologically reliant regardless of industry. Small and medium businesses are equally facing data and security challenges similar to large corporations coupled with other operational hurdles such as high operative costs, unmanageable workloads and limited access to a quality talent pool. Having cybersecurity resilience and a fortified information security system at place is one less thing to worry about.

## **Our Care**

To overcome customary challenges and build a better cybersecurity system that ultimately protects and secures data, we are certified and compliant with:

- ISO 27001:2013 and ISO 9001:2015
- General Data Protection Regulation (GDPR)
- Philippine Data Privacy Act of 2012
- Health Insurance Portability and Accountability Act (HIPAA)

Your company and client's data are safe with us. Our operations and associated client information are housed in state-of-the-art facilities with controlled access areas that provide 24/7 security.

Our comprehensive information security & data protection process ensures that all company and information is ultimately safe at all times. Regular risk assessments and audits are conducted to identify processes and procedures vulnerabilities that your company may be exposed to malicious gains both digitally and non-digitally. Strict measures are in place that prevent any unauthorized access of client's data at all times.

## **Pillars of Success: PPTS (People, Process, Technology, Security)**

Having established **People, Process, Technology, and Security** Pillars in place, your company can look forward to a fortified and well-executed cybersecurity and cloud management processes and strategy to help you focus on your business goals. Our VP for Sales and Marketing believes that,



“ I’ve been in the outsourcing business for many years and Infnit-O has by far the strongest data privacy and compliance process that I’ve experienced. Over the past 3 years, Infnit-O has established best practices in data privacy protection. And I’m proud to share that we built formidable processes to guarantee our continued effort in protecting our client’s data and information. ”

- Mike Gunion  
Vice President, Sales & Marketing

## People

Infnit-O aims to create long lasting partnerships and endless opportunities for our client’s business to grow by building a great team of experts that responds to their unique needs. The A+ teams we’re building have undergone a comprehensive recruitment process to identify the best people for our clients with the right mix of technical skills and up to date training.

We also have a solid **5-step Comprehensive Recruitment Process** that helps us build these great teams:

1. Human Aspect Assessment  
Analytical • Emotional • Spiritual • Intelligence Quotient
2. Applicant Credentials Verification  
Detailed review of work experience
3. 3-Level Interview Process  
Comprehensive independent interviews
4. Stringent Reference and Background checks
5. Robust Onboarding Process

Our team members have undergone necessary security and compliance training (i.e. HIPAA compliance training and Information Security Awareness courses) and other mandatory certifications to make sure that they are qualified for the role. We also conduct quarterly compliance audits and awareness checks to corroborate that our team members are always updated

with the latest policies. Information security modules and online courses are available for them as part of their growth and development efforts.

## Process

We render a strong understanding of information security processes all utilizing the latest technology to provide excellent value for our clients. We also have payroll processing, performance monitoring, project management, monthly and quarterly key performance updates and consultancy processes in place to make sure that not only cybersecurity concerns are addressed but also operational support is given. Our Quality Information Security Monitoring Management System (QISMMS) is a tool designed to monitor security compliance across our company. This was created to guarantee our organizations consistent conformity with information security.

## Technology

Our salient technologic setup such as customized workspaces, advance dialer system, call monitoring and recording and 24/7 IT support access adds another layer of security for clients. We have designed not just work at the office set up but also an effective remote work technology allowing necessary tools and IT support available in a work from home environment as part of our business continuity efforts. Tools proficiency for different services is also on top of our technological advancement. We support clients with the different softwares and applications for their business and other essential hardware support to ensure their internal processes are smoothly covered.

Any potential risks identified are then coordinated with the client immediately so we can work in guiding them resolving such risk.

## Security

Fortifying our security system through the cybersecurity insurance coverage, IT and data security, established information security, breach reporting process, incident handling process and being ISO-certified,

HIPAA-compliant and GDPR-compliant allows us to safeguard our clients' information safely with us. We believe that these security efforts are not only for data protection but also giving our clients peace of mind.

your data,  
our care.

## PEOPLE

- Sourcing, testing & hiring for fit
- Onsite and remote work models
- Highly efficient onboarding
- 24/7/365 Operations experienced, global leadership
- Deep functional expertise
- Hands-on HR support
- Adaptive Learning Programs
- Retention Programs
- Wellness Program (Physical, Mental, Social, Financial)
- Highly engaged team members

## PROCESS

- Seamless implementation
- Client project management
- Performance guarantee via KPI
- Performance Management
- Transparent KPI reporting
- Net Promoter Score metrics
- BCP options
- Continuous improvement expectations
- Customized client governance
- Consulting: process optimization and automation
- Collaboration and communication tools
- Stringent remote work standards

## TECHNOLOGY

- 24/7 Global IT Support
- Workstation/computer/headset
- Multi platform expertise
- Technology agnostic
- Triple redundant internet access\*
- UPS and APS\*
- Training Facilities (& Virtual)
- Meeting Rooms

\* Office-based

## SECURITY

- Comprehensive security measures to protect data, hardware, networks, virus/malware, physical protections
- Remote management and continuous security awareness
- Globally recognized security certifications: ISO9001, ISO27001
- Adherence to privacy laws: GDPR, DPA2012, HIPAA compliance





## Network and Application Layer Security

Having a layered security model allows us to support essential cyber and information security needs of our clients and consider network security as a fundamental element in safeguarding our partner's company data. We adhere to next-generation firewalls and enterprise-grade protection systems to limit and eradicate untrusted access to sensitive and secured information. We also have a **Company Policy & Procedure Manual Network Control and Security** as our bible to set the seal of network security.

Infinet-O systems are protected using the combination of the following:

### Network Perimeter Level

- Palo Alto next generation firewall & IDS
  - Intrusion Detection/Prevention system
  - Gateway Antivirus
  - Internet Access control (Blacklist/Whitelist/File Download Blocking)
  - Application Level Control
  - Botnet Correlation and Identification
- Site to site and/or client based VPN connectivity with 2FA authentication
- SSL based connections and Web application firewall

### Endpoint Level

- Individual username and password through Microsoft Active Directory and Group Policy
- Two-Factor Authentication via physical dongles (Yubikey)
- Symantec Endpoint Protection (Antivirus/Antimalware and Network Threat Protection)
- Full Disk encryption
- Peripheral access control ( USB , Printers)

### Proactive Security

One of our ultimate goals is to prevent our clients from experiencing security breach by setting up proactive security measures and anticipating potential situations to save our clients from experiencing cybersecurity threats and attacks that can lead to compromise and crippling loss. Infinet-O continuously monitors its security posture through the following activities:

- Automatic Patch Management Systems for OS and 3rd party apps (Manage Engine Desktop Central)
- Vulnerability Assessment (Tenable:Nessus)
- Penetration Testing (Rapid7:Metasploit )
- Information Security Awareness Programs
- Internal and External Security Audits



## Data Privacy

Privacy principle is tantamount with our information security objectives because we know that this implements strong security measures that reduces privacy breaches. Fewer breaches strengthens the trust and bond we strive to seal with our partners at the same time providing them with peace of mind while they achieve their business goals. We also value ethical trust bestowed upon us by responsibly handling confidential information of our clients. According to a study conducted by [Ponemon](#), 65% lose trust in the organization if their personal data was breached.

Infinit-O currently adheres to Philippines Data Privacy Law and have the following alongside with:

- Appointed a Data Privacy Officer (primary contact)
- Privacy Impact Risk Assessment (Per group and project)
- Established Information security and privacy policies
- Breach reporting process

## Incident Handling

At Infinit-O, we have a quick incident handling response to mitigate vulnerabilities and reduce risks posed from any security incidents. We value our partner's trust that is why regardless of the severity of the breach, we have a strong incident response plan in place. This strategy addresses security incidents, the investigation process and how it is communicated to the questioned party, and the notification requirements following a data breach. Our incident handling plan is designed to instill confidence in our clients and protect their target revenue by eliminating potential loss from compromised data.

Infinit-O has developed a tool/system to handle both information security/privacy

and quality related issues or incidents. (QISMMS)









- Investigation of the event/offense
- Incident report
- Root-Cause Analysis by the Incident Handling Team reflect 4 pillars (People, Process, Technology and Security)
- Incident handling team
- Data Privacy Officer
- IT Director
- Management Committee

## Remote Work

The digital climate has also brought a major change to many traditional companies by transitioning to working from home as a more stable and permanent change rather than a temporary effort. A [survey](#) from a global research company, Gartner, gathered from 317 CFOs and business finance leaders found out that 74% plan to move their previously on-site workforce to permanent remote positions.

As more organizations are relying on technology to enable work to happen seamlessly, cyber criminals are lurking to attack. We acknowledge the necessity of having a secured remote work set up, thus, we responded by fortifying our remote process and measures. Our team members that are working from home are provided with company computers and laptops that are setup with standard security requirements like, Active Directory Membership for authentication and configuration, Full disk encryption, Firewall, Antivirus/Antimalware software and Two factor authentication.




Other remote work optimization includes:

Security Categories	Security Features	Local Office Computers	Remote Office Computers
 Hardware Access Protection	Password Protected Login	✓	✓
	Two-Factor Authentication	✓	✓
 Physical Protection	Access Controlled Areas: Dedicated Home workspace	✓	✗
	CCTV Monitoring and Recording	✓	✗
 Hardware Data Protection	Computer Hardening	✓	✓
	USB Port's Disabled	✓	✓
	Printer Access Controlled	✓	✓
	Full Disk Encryption	✓	✓
	Automated File Deletion Scripts	✓	✓
 End-Point Virus and Malware Protection	Realtime Antivirus Monitoring	✓	✓
	Realtime Anti-Malware Monitoring	✓	✓
	Automatic Virus Definition Updates	✓	✓
	Forced Scanning	✓	✓
	End-Point-Based Intrusion Prevention Systems	✓	✓
 Patch Management	Automated Operating System Updates	✓	✓
	Automated Application and 3rd party Updates	✓	✓
	Automated Driver Updates	✓	✓
 Email Protection	2FA Login	✓	✓
	Attachment Automated Virus Scan	✓	✓
	Antispam	✓	✓
 Network Protection	WebServices Whitelis/Blacklist Access: Via VPN	✓	✗
	Network Based Intrusion and Prevention System: See Centrally managed Endpoint Based Intrusion Prevention system	✓	✗
	Network-Based Firewall	✓	✗
	Computer Firewall	✓	✓
 Remote Management and Security Awareness	Information Security and Privacy Training	✓	✓
	Remote Work Security Training	✓	Enhanced Coverage
	Remote Monitoring Software	✗	✓



## HIPAA Compliance

Ignorance with the rule or failure to comply can result in multiple million-dollar fines especially for healthcare organizations and other HIPAA-covered entities. Infnit-O assures that we preserve and protect sensitive and personal information of our partners and their clients by reducing healthcare fraud and abuse, enforcing standard health information and guaranteeing security and privacy of health information through HIPAA compliance. We value a national standard to protect individuals' medical records and other personal health information through confidentiality and security initiatives.

HIPAA Security Checklist	Compliance	Monitoring
<p>Ensure proper configuration of devices that access company and client data (i.e., are encrypted, with password, firewall, and antivirus protection)</p>	<p>Computers &amp; laptops were provided to team members that are set-up with standard security requirements:</p> <ul style="list-style-type: none"> <li>• Active Directory Membership</li> <li>• Full Disk Encryption</li> <li>• Firewall</li> <li>• Antivirus/Antimalware Software</li> <li>• Two-factor authentication</li> </ul>	<p>Installing remote management software for Infnit-O IT team to monitor and deploy security patches and update firewall configurations regularly</p>
 <p>Secure home networks (i.e routers, dongle, etc.) and working area</p>	<ul style="list-style-type: none"> <li>• Launched mandatory security awareness courses for all team members</li> <li>• Information drive for security-related resource material for latest trends &amp; updates</li> <li>• Submission of IT &amp; security checklist to team members to meet the remote work set up technical requirements</li> <li>• Teleworking and Mobile Device Policy in place wherein team members who must connect via Wi-Fi will utilize WPA2 standard (as minimum) and adhering to Infnit-O password provisions</li> </ul>	<ul style="list-style-type: none"> <li>• Automated completion reports notification email to managers for compliance monitoring</li> <li>• Quarterly Infosec &amp; Data Privacy awareness quiz for all team members</li> </ul>
<p>Encrypt password-protect on devices employees use to access PHI remotely</p>	<p>Supplying company computers and laptops with full disk encryption enabled by native Microsoft Bitlocker or IOS Filevault</p>	<p>Installation of remote management software which allows Infnit-O to monitor and audit full disk encryption status</p>
 <p>Configuration of devices for home use</p>	<p>Automatically filtering devices prior to connecting to VPN servers and before granting access to Infnit-O's network.</p> <p>Checking the following presense:</p> <ul style="list-style-type: none"> <li><b>A.</b> OS version and security patch details</li> <li><b>B.</b> Company antivirus software with latest definition and most recent scan requirement</li> <li><b>C.</b> Firewall will be enabled</li> <li><b>D.</b> Full disk encryption</li> </ul>	<ul style="list-style-type: none"> <li>• Firewall and VPN systems automatically allows connection if devices pass the security requirement and block it if otherwise</li> <li>• An alert notification will be sent to Infnit-O's security team if an attempt to connect is made but not passing the authentication requirements for further investigation</li> </ul>
 <p>Encryption of PHI before transmission</p>	<ul style="list-style-type: none"> <li>• Method of transmission is agreed upon with the clients/vendors beforehand. Normally transmitted via our servers or cloud-based file sharing with end-to-end encryption protocols.</li> <li>• EHPI files are encrypted and password protected prior to sending to secured channels.</li> </ul>	<p>Email servers and cloud-based sharing are regularly audited by 3rd party firms to ensure HIPAA compliance</p>
<p>Develop policies and procedures prohibiting employees from allowing friends and family from using devices that contain PHI</p>	<p>Adhering to Infnit-O Teleworking and Mobile Device Policy wherein users working remotely will not allow access of company property to unauthorized users like family and friends</p>	<ul style="list-style-type: none"> <li>• Team members are required to read and sign off our Acceptable Usage policies</li> <li>• Automatic locked out system for devices inactive for a 8 minutes</li> </ul>

## HIPAA Security Checklist



## Compliance

## Monitoring

Signing of Confidentiality Agreement for employees

Infinet-O team members are required to sign an NDA & other network acceptable usage policies as part of the contract

Regular exams are conducted to monitor security awareness level

Bring Your Own Device (BYOD) Agreement are signed with clear usage rules

That the work equipment will have security & communication software installed and will be used for work purposes only.

Installation of remote management software which allows Infinet-O to monitor and audit full disk encryption status



Provide file cabinets with locks or safes for employees who store hard copy (paper) PHI in their home offices

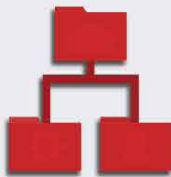
With the remote set up, no lockers are provided but printing and USB access are disabled on all remote computers

Printing and USB/device connections are controlled through Windows Active directory Group Policies and Symantec endpoint protection software

Email notifications are sent out in case team members plug in unauthorized devices (e.g. USB disk, printers) to IT security team for further investigation and proper sanctions

Providing HIPAA-compliant shredders for remote workers for proper disposal of PHI hard copies

Paper shredders are not provided but the Control of Records Policy outlines how to protect PHI hard copies



Adherence on Media Sanitization Policy

Control of Records Policy includes the secure and reliable disposal (i.e., shredding, destruction) of any media containing company information.

IT Disposal policy states that all non-operational disk / removable media will be physically destroyed while all operational disk/removable media drives must be erased via military grade multiple overwriting process application or through use of disk nuking software.

Asset disposal request and media sanitization reports are submitted accordingly

Employees will disconnect from the company network at the end of their shift through IT configuring timeouts

End users are disconnected automatically from corporate VPN networks after 15 minutes of inactivity.

Reauthentication is needed to reconnect to the VPN.

Maintain and periodically review logs of remote access activity

Firewall/VPN systems automatically collects and logs remote connections and network activities.

Regular review of access and VPN logs by the IT security team

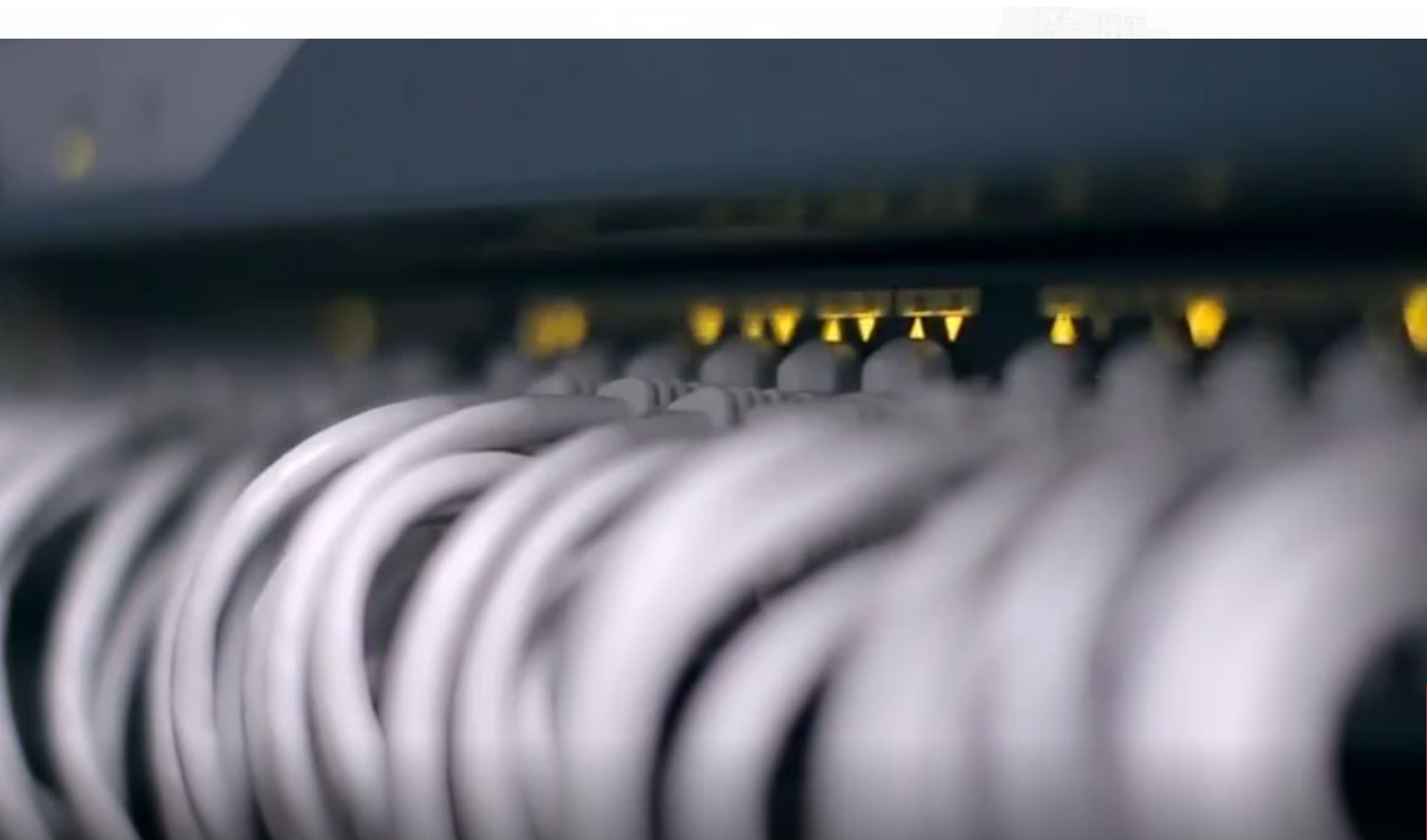




## Information Security Video

With Infinit-O's proactive security system, we cover and secure your business' sensitive data at every endpoint within our company. We provide a robust and world-class information security and data management process.

Know more about our information security measures. Click the image to watch the video.



## Key Benefits

A partnership with Infinit-O will aid you in building a great team of cybersecurity and cloud experts, having a well-build and fortified information security process but also create long lasting partnerships and endless opportunities with these key benefits:

### Cost Reduction

Expect high quality & productivity with a 70% savings on operational costs.

### Scalability

As your business demands shift, so can your Infinit-O team.

### Access to Excellent Talent

Our world-class "A+ Recruiting" process attracts world-class talent, with an industry-leading retention rate.

### Operational Excellence

Collaborative Service Level Agreement, metrics-intensive performance, and open communication.

### Trusted Partnership

Have confidence with our >97% client retention rate and 72 NPS score.  
ISO 27001 and 9001 certified, GDPR, HIPAA and DPA2012-compliant



Let's build a great, high-performing team specifically designed to meet your unique needs

start small  
exceed expectations  
think infinitely  
think **INFINIT-O**

To know more about us, click:



Website



Call Us