

Privacy Statement

OneNeck® IT Solutions LLC is dedicated to providing superior customer satisfaction and to safeguarding personal information about our clients and employees. When we collect Confidential Personal Information about you, we will inform you in clear and conspicuous language of the purpose for which we are collecting and/or using the information, any third-parties to whom we will disclose the information, the choices you have regarding limiting the use and disclosure of your information, and how you may contact OneNeck to review, correct, or dispute this information.

We will use your Confidential Personal Information only in ways that are compatible with the purposes for which we collected it from you or which you subsequently authorized, and we will provide you with notice before we use or disclose your information for a purpose other than that for which it was originally collected. We will take reasonable steps to ensure that all Confidential Personal Information we collect, retain, or use is relevant to its intended use, accurate, complete, and current.

When we host data for customers, we start with two simple principles:

- We use, disclose, and otherwise process personal data only to provide the services requested by our customer.
- We maintain robust security to protect it against unauthorized acquisition or use.

OneNeck's obligations with respect to personal data for which OneNeck is a data processor, such as data that OneNeck hosts for its customers, are further defined in OneNeck's agreements with its customers. Personal information obtained from our clients is processed in compliance with the terms and conditions set forth in our client contracts and correspondence and our professional standards.

OneNeck recognizes that its commercial customers may also be subject to detailed privacy and information security regulations as a financial institution under the Gramm Leach Bliley Act or as a covered entity or business associate under HIPAA. We can readily accommodate legal requirements to ensure appropriate privacy controls, and we enter into additional agreements, such as Business Associate Agreements, when required by applicable law.

Business with personal data originating in the European Union should rest assured that OneNeck complies with the data protection requirements applicable to it.

OneNeck complies with the EU – U.S. Privacy Shield Framework, as set forth by the U.S. Department of Commerce in consultation with the European Commission, regarding the collection, use and retention of personal data received from the European Union. OneNeck annually certifies its adherence to the Privacy Shield Principles of notice; choice; accountability for onward transfer; security; data integrity

and purpose limitation; access; and recourse, enforcement and liability. To learn more about the EU – U.S. Privacy Shield Framework, please visit <https://www.privacyshield.gov/EU-US-Framework>. To view OneNeck's certification, please visit <https://www.privacyshield.gov/list>.

OUR COMMITMENT TO PROTECTING CUSTOMER PRIVACY

OneNeck® IT Solutions LLC supports the operations of its affiliates, ONENECK DATA CENTER HOLDINGS, LLC and ONENECK IT SERVICES CORPORATION (collectively "OneNeck"). This Privacy Statement applies to each of the OneNeck entities.

OneNeck also requires any third party service provider with whom we share or collect Confidential Personal Information, such as our agents, vendors, suppliers, subcontractors, and independent contractors, to provide written assurances that they provide privacy protections substantially similar to those provided in this Privacy Statement and the EU – U.S. Privacy Shield Framework for personal data concerning citizens of the European Union. OneNeck is responsible for ensuring that such third party service providers process personal data from the EU in a manner consistent with the Privacy Shield Principles.

This Privacy Statement does not apply to services, products, or Web sites that do not display or link to this Privacy Statement or that have their own privacy statements.

By subscribing to our services or accessing our Web sites, you agree to our collection, use, disclosure and other processing of personal data as described in this Privacy Statement.

COLLECTION OF YOUR CONFIDENTIAL PERSONAL INFORMATION

When we collect Confidential Personal Information about you, we will inform you in clear and conspicuous language of the purpose for which we are collecting and/or using the information, any third-parties to whom we will disclose the information, the choices you have regarding limiting the use and disclosure of your information, and how you may contact OneNeck. We also will provide you with notice before we use or disclose your information for a purpose other than that for which it was originally collected.

Confidential Personal Information is information that relates to you and identifies or can be used to identify you. This information includes your name, billing address, social security number, driver's license number, credit card number, bank account number, email address, and credit information. We may also collect and host the Confidential Personal Information contained in the data that you store on our site. TDS

may collect Confidential Personal Information for those purposes specified in this Privacy Statement, and as otherwise permitted by law.

We may collect Confidential Personal Information through a business office, over the phone, or online. You may choose to provide this information to us through a number of interactions such as by:

- Ordering a product or service from us
- Sending us an email
- Registering to receive information about our products or services
- Responding to customer service inquiries
- Applying for a job or a grant, or
- Entering a contest.

We may also collect this information about you from trusted agents who are authorized to sell our products and services, or from employees of our Affiliates. Affiliates refers to any of the Telephone and Data Systems, Inc. owned companies. When we receive personal information from Affiliates, we will use and disclose such information in accordance with the notices provided by those entities and the choices made by the individuals to whom such personal information relates.

We may also collect Confidential Personal Information about you that helps us better serve your special needs and interests, such as when you respond to questions, surveys or other customer service related inquiries. You can always choose not to provide certain Confidential Personal Information to us, but we may not be able to provide you with certain services or features as a result.

For training or quality assurance, we may also monitor or record our customer service calls with you.

SENSITIVE PERSONAL DATA

We do not generally collect sensitive personal data, including personal data about personality and private life, racial or ethnic origin, nationality, political opinions, membership of political parties or movements, religious, philosophical or other similar beliefs, membership of a trade union or profession or trade association, physical or mental health, genetic code, addictions, sexual life, property matters or criminal record (including information about suspected criminal activities). You are not required to provide any Sensitive Personal Data to use any of our services.

If you choose to provide us with unsolicited sensitive personal data, you consent to our using the data subject to applicable law as described in this Privacy Statement. For sensitive personal data, OneNeck will give individuals the opportunity to provide affirmative and express (opt-in) consent to the disclosure of the data to a non-agent

third party or to the use of their data for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

Sensitive personal data is also afforded all protections we provide to Confidential Personal Information generally.

TECHNICAL INFORMATION AND COOKIE POLICY

As part of network operations and when you visit a OneNeck Web site, we may automatically collect certain information such as your domain type, your IP address, and click stream information to gauge the effectiveness of our Web sites, improve our online operations, enhance your online experience with customized content, and focus our marketing efforts to better meet the needs of our customers.

We may store small data files known as cookies, or other similar technologies, on your computer or mobile browser when you visit one of our Web sites. Cookies allow us to personalize and protect your service by collecting and storing information that will identify you when you visit a Web site. Cookies also allow us to collect 'Web site usage' information when you visit our Web sites, including IP address, Web browser and operating system types, Web pages visited on our Web sites, time spent on our Web pages, and return visits to our Web sites. We may combine the Web site usage information with your Confidential Personal Information in order to provide a more customized online experience to you and to provide advertising about goods and services that may be of particular interest to you. These same cookies may also be used by our advertising partners on TDS and other Web sites to display advertisements based on the preferences you demonstrate through your online activities. We do not track user click stream or other information resulting from activity on sites that are not operated by TDS. For further information about how to opt-out of behavioral advertising on the Internet, please see <http://www.networkadvertising.org/choices/>.

You may be able to disable cookies on your computer; however if you do so, you may limit your experience on this Web site. You can set your browser to delete cookies or to tell you before you accept one. Look in your browser's Options or Preferences menu for settings relating to cookies.

“Do Not Track” signals are options available on your browser to tell operators of websites that you do not wish to have your online activity tracked. Our websites operate no differently if these “Do Not Track” signals are enabled or disabled. Our Internet Services do not allow any third parties to collect Personal Information about your online activities over time or across websites for their own purposes.

OneNeck is not responsible for the practices, including the use of cookies, employed by third party Web sites linked to or from our Web site or for the content contained

therein. The Web sites and services you are able to access on the Internet are outside the control and limits of this Privacy Statement.

OneNeck may link to other outside Web sites but it is not responsible for the privacy practices of these other sites. You should check their privacy policies (if available) before submitting any personal information since the privacy practices of these other sites may be different from ours. You should be aware that any personal information collected on these other sites is collected by that third party Web site and is governed by that site's policy.

USE OF YOUR CONFIDENTIAL PERSONAL INFORMATION/ DATA INTEGRITY

We will use your Confidential Personal Information only in ways that are compatible with the purposes for which we collected it from you or which you subsequently authorized. We will take reasonable steps to ensure that all Confidential Personal Information we collect, retain, or use is relevant to its intended use, accurate, complete, and current.

We may use your Confidential Personal Information to provide you with and manage the services you request, communicate with you to maintain customer relations or to suggest new products and services that may be of interest to you, personalize the content we deliver, conduct industry or consumer surveys, manage, improve and troubleshoot our network and services, enforce our Terms of Service, or for any purpose otherwise permitted or required by law.

When you want to set up an account with OneNeck, in order to determine your credit worthiness, we may use some of your Confidential Personal Information to request a credit report from a credit-reporting agency based on a permissible purpose consistent with the Fair Credit Reporting Act.

OneNeck uses the information collected on its Web sites to provide you with the information you requested. When you use our Web sites to order products or services, or to request information about them, we may use the information we have about you as we would use the same information obtained offline - for example, to evaluate your service needs and contact you regarding additional services you may find useful. You may also submit applications for employment online, and we will use the information you provide to consider you for employment.

We will not use your Confidential Personal Information for a purpose other than the purpose for which it was originally collected or subsequently authorized without your consent. We will not use sensitive personal information for a purpose other than the purpose for which it was originally collected or subsequently authorized unless you have provided your affirmative and express (opt-in) consent.

When you provide us with your Confidential Personal Information, we collect that certain purposes that are required or permitted by applicable law, and OneNeck may access or disclose Confidential Personal Information without further notice or your consent in order to: (i) investigate, protect or defend the legal rights or property of TDS, OneNeck, our Affiliated Companies or their employees, agents and contractors (including enforcement of our agreements); (ii) protect the safety and security of customers or members of the public including acting in urgent circumstances; (iii) protect against fraud or for risk management purposes; or (iv) comply with the law or legal process such as a subpoena. OneNeck will provide its customers with prompt notice of law enforcement requests or demands for their data to the fullest extent allowed by applicable law so that the customer may assert any defenses or other legal interests that it wishes.

If TDS or OneNeck sells all or part of its business or makes a sale or transfer of all or a material part of its assets or is otherwise involved in a merger, transfer, or liquidation of all or a material part of its business, your Confidential Personal Information may be transferred to the party or parties involved in the transaction.

If we obtain Confidential Personal Information from a Third Party, our use of that information is also governed by this Privacy Statement.

If you submit an employment application, resume or similar information about yourself, it will be used only for the purpose of considering you for employment or such other purpose as requested by you.

COLLECTION AND USE OF CHILDREN'S CONFIDENTIAL PERSONAL INFORMATION

OneNeck sites and services are intended for adults. In order to respect the privacy of children online, OneNeck does not knowingly collect, maintain or process Confidential Personal Information submitted by children under the age of 18, and we will promptly delete any such information when we become aware that it was collected inadvertently.

If we do collect age information, and users identify themselves as under the age of 18, the site will block such users from providing Confidential Personal Information.

SHARING OF YOUR CONFIDENTIAL PERSONAL INFORMATION / ONWARD TRANSFER

We will not disclose your Confidential Personal Information without your consent outside of TDS, OneNeck, its Affiliates, or its authorized agents, such as service

providers who help initiate, render, bill and collect for our products and services, other than as described in this Privacy Statement. No data that we host or process for our clients is used for our marketing purposes or the marketing purposes of any other party.

We will not share or sell any Confidential Personal Information collected through the OneNeck with any external parties without your consent. Confidential Personal Information that we collect from you may be shared with Affiliates and Third Parties with consent for the purposes of marketing our products and services. Depending on the circumstance, notice and opt-out may be a permissible means of obtaining your consent. OneNeck may sell your Confidential Personal Information to Third Parties in order to enforce our rights under the Terms of Service. For example, we may sell past-due accounts receivable in an effort to collect for unpaid services. OneNeck will obtain written assurances from its agents that they will safeguard Confidential Personal Information consistently with this Statement. Affiliates and Third Parties are permitted to obtain only the Confidential Personal Information they need and are prohibited from using it for any purpose other than those permitted by law or with your consent. When we use service providers to assist us in processing your Confidential Personal Information, we require that they comply with this Privacy Statement and maintain appropriate privacy and security measures. Where we have knowledge that a Third Party is using or disclosing Confidential Personal Information in a manner contrary to this Statement, OneNeck will take reasonable steps to prevent or stop the use or disclosure.

ACCESSING YOUR CONFIDENTIAL PERSONAL INFORMATION

OneNeck takes reasonable measures to assure that the Confidential Personal Information we use about you is reliable, accurate, complete, and up-to-date. Customers who wish to review and/or edit their Confidential Personal Information may do so by contacting us using the information listed at the end of this statement. We will make reasonable good faith efforts to provide you with access to your Confidential Personal Information upon request either to correct or amend this data if it is inaccurate or incomplete or to delete such data at your request if it is not otherwise required to be retained by law or for legitimate business purposes.

We may decline to process requests for information that are unreasonably repetitive or systematic, require disproportionate technical effort, jeopardize the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes), or for which access is not otherwise required. In any case where we provide information access and correction, we perform this service free of charge, except if doing so would require a disproportionate effort.

OneNeck provides customers with the ability to authorize individuals ("Authorized User") to make inquiries, limited changes, or both, in order to maintain their account.

Customers may specify the type of information and changes that the Authorized User is approved to request. Customers may add or remove an Authorized User from their account at any time.

We ask customers and their Authorized Users to identify themselves and the information requested to be accessed, corrected or removed before processing such requests. If you or your Authorized User contacts us via phone, you will be asked to provide your name, the account Personal Identification Number ("PIN") (if the account is PIN protected; otherwise you will be asked to provide other information for the purposes of identity verification), and the billing address ZIP code before we are able to assist you. You or your Authorized user will be asked to present a valid photo ID when requesting account information while at a business office.

COMMUNICATION PREFERENCES

If you do not want OneNeck to use your Confidential Personal Information to contact you for marketing or solicitation purposes (excluding notices about your existing account), OneNeck customers may make this request to privacy@tdshms.com. When writing to us, please specify which contact methods (phone calls, mail, bill inserts, or email messages) you would prefer that we do not use to communicate to you for the purposes outlined above. Keep in mind that restricting contact methods may make it more difficult for us to keep you informed about new products and services that can be of benefit to you. You can revoke these options at any time by contacting us using one of the methods provided in this Privacy Statement.

These choices do not apply to the display of online advertising or the receipt of transactional and service communications that are considered part of certain OneNeck services, which you may receive periodically unless you cancel the service.

If you request to not be contacted by phone for marketing or sales purposes, please note that the TDS Do Not Call List restricts these types of phone contacts from TDS only, so you may continue to receive calls from other companies. If you would like to add your number to the National Do Not Call List, you may do so by calling 1-888-382-1222 or visiting www.donotcall.gov.

CONTROLLING UNSOLICITED EMAIL ("SPAM")

OneNeck is concerned about controlling unsolicited email or "spam." While OneNeck and its vendors continue to actively review and implement new technology to help prevent this activity, there is no currently available technology that will totally prevent the sending and receiving of unsolicited email. Using junk email tools and being cautious about the sharing of your email address while online will help reduce the amount of unsolicited email you receive. For more information about this and other

related topics go to the Federal Trade Commission's website at <http://www.onguardonline.gov>.

SECURITY OF YOUR CONFIDENTIAL PERSONAL INFORMATION

OneNeck leverages ITIL based practices to manage mission critical data centers and customer infrastructure 24x7x365. Our facilities are [SSAE 16](#) audited to ensure that independent reviewers conclude that our customers' data is secure, available, and compliant up to these rigorous industry standards.

OneNeck has designed these and other reasonable technical and organizational security safeguards to protect against such risks as loss or unauthorized access, destruction, use, alteration, modification, or disclosure of Confidential Personal Information. You should understand that the open nature of the Internet is such that data may flow over networks without security measures and may be accessed and used by people other than those for whom the data is intended. Cybersecurity threats are also constantly evolving, and while we strive to maintain robust protections, no one can guarantee the absolute security of data accessible via the Internet.

Our policies restrict access to Confidential Personal Information to OneNeck employees, employees of our Affiliates, and authorized Third Parties who need to know that information in order to operate, develop or improve our services; and our policies require that these individuals be bound by confidentiality obligations and may be subject to discipline, including termination, if they fail to meet these obligations. We do not guarantee that our safeguards will always work.

Our policies require us not to store Confidential Personal Information beyond what is necessary for business purposes, including for internal service evaluation and quality assurance purposes, except as otherwise required by law.

ENFORCEMENT OF THIS PRIVACY STATEMENT

OneNeck conducts compliance audits of our relevant privacy practices to verify adherence to this Privacy Statement. Any employee that OneNeck determines is in violation of this Statement may be subject to disciplinary action up to and including termination of employment.

Our employees, agents, and Affiliates are trained regarding their responsibilities to safeguard your privacy. They are required to adhere to a Code of Business Conduct, this Privacy Statement, and OneNeck's policies which support our commitment to protecting customer privacy. If employees or Third Parties become aware of practices that raise privacy concerns, they are required to report them to their supervisors or to contact OneNeck's Incident Response Team.

PRIVACY SHIELD COMPLIANCE

OneNeck complies with the EU – U.S. Privacy Shield Framework regarding the collection, use, and retention of personal information from the European Union. OneNeck has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement with respect to all personal data transferred from the EU to the US within the scope of its certification. To learn more about the EU – U.S. Privacy Shield Framework, and to view OneNeck's certification, please visit <https://www.privacyshield.gov/list>.

CALIFORNIA PRIVACY RIGHTS

A business subject to California Civil Code section 1798.83 is required to disclose to its customers, upon request, the identity of any Third Parties to whom the business has disclosed "personal information" regarding that customer within the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to:

OneNeck IT Solutions Attn: Legal Dept. 525 Junction Road Madison, WI 53717

Please note that California businesses are only required to respond to a customer request once during the course of any calendar year.

CHANGES TO THIS PRIVACY STATEMENT

We will occasionally update this Privacy Statement to reflect changes in our services and customer feedback or in legal requirements. When we post changes to this Privacy Statement, we will revise the "last updated" date at the top of this Privacy Statement. If there are material changes to this Privacy Statement or in how OneNeck will use your Confidential Personal Information, we will make reasonable attempts to notify you directly. We encourage you to periodically review this Privacy Statement.

DISPUTE RESOLUTION

Any questions or concerns regarding the use or disclosure of Confidential Personal Information should be directed to OneNeck at the address given below. OneNeck will investigate and attempt to resolve disputes regarding use and disclosure of personal information by reference to the principles contained in this Statement. If you are unsatisfied with the way we have responded to any concerns about our handling of personal information about you, the matter may be dealt with through the American

Arbitration Association for all personal data, except that any disputes involving personal data from the European Union must follow the procedures below.

OneNeck voluntarily complies with the EU – U.S. Privacy Shield Framework and is subject to the investigatory and enforcement powers of the Federal Trade Commission.

Any person in the EU who is not satisfied with OneNeck’s compliance with the EU – U.S. Privacy Shield may contact OneNeck by mail at: OneNeck IT Solutions Attn: Legal Dept. 525 Junction Road Madison, WI 53717 or by email at: legal@OneNeck.com to resolve such complaints. If you believe that such a complaint has not been resolved, you may first try to settle the dispute by mediation, administered by the International Centre for Dispute Resolution under its Mediation Rules, before resorting to arbitration, litigation, or some other dispute resolution procedure. The rules governing these procedures and information regarding how to file a claim free of charge can be found here: <http://info.adr.org/safeharbor/>. If you remain dissatisfied, you may contact your national Data Protection Authority in the country where you reside. OneNeck agrees to cooperate and comply with the Department of Commerce in resolving such disputes. If you remain dissatisfied and meet the pre-arbitration requirements of Annex I Part C of the EU – U.S. Privacy Shield Framework, you may invoke binding arbitration pursuant to procedures in Annex I of the EU – U.S. Privacy Shield Framework Principles found here: <https://www.privacyshield.gov/EU-US-Framework>.

CONTACTING US

OneNeck welcomes your comments regarding this Privacy Statement. If you have questions about this Privacy Statement or believe that we have not adhered to it, please contact us by writing to us at the following address:

OneNeck IT Solutions Attn: Legal Dept. 525 Junction Road Madison, WI 53717

Any questions or concerns regarding the use or disclosure of personal information should be directed to OneNeck at the address given above.

Last Update: 11/14/2017