EmeSec Privacy Policy

1 EmeSec Privacy Statement

EmeSec aims to ensure that individuals are aware that their data is being processed, that they understand how the data is being used, and how to exercise their rights.

To that regard, EmeSec's privacy policy sets out how individual's data is being used by EmeSec.

EmeSec privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with us – including, but not limited to: employees, staff, customers, and website visitors.

- EmeSec will protect your privacy and keep personal information safe. EmeSec uses encryption tools and other security safeguards to protect personal data.
- EmeSec will not sell your personal information to anyone, for any purpose.
- EmeSec will fully disclose its privacy policy in plain language and make our policy accessible on as needed basis.
- EmeSec will notify you of revisions to our privacy policy
- You have choices about how EmeSec uses your information for marketing purposes, you are in control and can opt out at any time.
- EmeSec wants to hear from you, send questions or feedback regarding EmeSec's privacy policy to privacy@emesec.net.

EmeSec requires individual's help in keeping your personal information accurate and up to date, so please notify us of any changes to your personal information. To update personal information and communication preferences, please contact us at privacy@emesec.net.

EmeSec makes a good faith effort to honor your reasonable requests to access and correct your data if it is inaccurate or delete the data if we are not required to retain it by policy, legitimate purpose, or law.

EmeSec may provide links to other third-party websites and services that are outside our control and not covered by this Privacy Policy. You are encouraged to review the privacy statements posted on those websites (and all websites) you visit.

2 Policy

This Privacy Policy describes how EmeSec collects, uses, discloses, transfers, stores, retains, or otherwise processes your information when you (whether "you" being a person or business) apply for employment, are an employee/staff member within EmeSec, or inquire about our services, etc. *Please read this Privacy Policy carefully and in its entirety*.

EmeSec is committed to maintaining your trust by protecting and safeguarding personal information that we may collect and use. This policy describes how personal data is collected, handled and stored to meet EmeSec's privacy protection standards, and to comply with the law.

EmeSec needs to occasionally gather and use certain information about individuals. Individuals may include, but are not limited to: customers, suppliers, business contacts, employees, staff members, and other people EmeSec has a relationship with or may need to contact.

This Privacy Policy ensures EmeSec:

- Complies with data protection laws and follows good practice;
- Protects the rights of staff, customers, and partners;
- Is open about how individual's data is stored; and
- Protects itself from the risks of a data breach.

3 PURPOSE

To comply with the law, personal information must be collected and used fairly; stored safely and not disclosed unlawfully.

Personal data must:

- Be processed fairly and lawfully;
- Be obtained for only specific, lawful purposes;
- Be adequate and relevant, yet not excessive;
- Be accurate and kept up to date;
- Not be held for any longer than necessary;
- Processed in accordance with the rights of data subjects;
- Be protected in appropriate ways; and
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection (applies only to data within the EU).

4 SCOPE

The policy applies to EmeSec Incorporated and all Users including, but not limited to; employees, staff, contractors, suppliers, and other people working for or on behalf of EmeSec.

It applies to all data that EmeSec holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act of 1998. This can include, but is not limited to:

- Names of individuals,
- Postal addresses,
- Email addresses,
- Telephone numbers, and
- Other information relating to individuals.

5 RESPONSIBILITIES

Everyone who works for or on behalf of EmeSec has the same responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have the key areas of responsibility:

The CEO is ultimately responsible for ensuring that EmeSec meets necessary legal obligations related to privacy.

The Data Protection Officer, or designee, is responsible for:

- Compliance with European data protection principles, i.e. processing data fairly and lawfully, and using data for specific, legitimate purposes;
- Keeping the CEO updated about data protection responsibilities, risks, and issues;
- Reviewing all data protection procedures and related policies, in line with agreed schedule;
- Arranging data protection training and advice for employees;
- Handling data protection questions for staff and anyone else covered by the policy; and
- Dealing with requests from individuals to see the data EmeSec hold about them.

The Data Controller (either alone or in conjunction with another person) determines the purposes and manner in which any personal data is to be processed. He or she is also responsible for:

- Compliance with European data protection principles, i.e., processing data fairly and lawfully, and using data for specific, legitimate purposes;
- Notifying the relevant national authority before carrying out any data processing;
- Providing certain information to individuals about whom EmeSec holds personal data, i.e., your identity, details of the data held and why the data is held/processed; and
- Implementing technical and organizational measures to protect personal data against accidental loss/destruction, unauthorized access or other unlawful processing.

IT Support is responsible for:

- Ensuring all systems, services, and equipment used for storing data meet applicable security standards;
- Performing periodic checks and scans to ensure security hardware and software is functioning properly; and
- Evaluating any third-party services that EmeSec is considering using to store or process data.

Marketing is responsible for:

- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries from journalists or media outlets; and
- Where necessary, working with staff to ensure marketing initiatives abide by data protection principles.

6 COLLECTION OF PERSONAL INFORMATION

EmeSec will inform you of the purpose for collecting personal information when we collect it and use it to fulfill the purposes for which it was collected, and as required by applicable laws for legitimate purposes. "Personal information" is any information that can be used to identify an individual, which may include name, address, email address, phone number, etc. We collect information, and engage third parties for collection of personal information to assist us for a variety of reasons, such as:

- Managing job applications,
- Enabling the use of certain features of our services,
- Personalizing your experience, and
- Collecting information provided by you.

If you choose to provide a third party's personal information (such as name, email, and phone number), we will assume that you have the third party's permission to provide us with the information. Examples include forwarding reference material to a friend or job references/referrals. This information will not be used to any other purpose.

Types of information we may collect from you includes, but not limited to;

- **Identifiable information.** Your name, email address, mailing address, phone number, photograph, birthdate, passport, driver's license, Social Security, taxpayer identification, or other government-issued identification; or other historical, contact, and demographic information when you apply for employment or sign up for EmeSec Services, signature and authentication credentials (i.e., information you use to login to your account(s)), including IP address.
- **Financial Information.** Information such as a bank account, credit reports, and other publicly available information.
- **Tax Information.** Withholding allowances and tax filing status.
- **Transaction Information.** When you use our services to make, accept, request, or record payments, we collect information about when and where the transaction occurs, the names of the transacting parties, a description of the transactions, the payment or transfer amounts, billing and shipping information and the devices and payment methods used to complete the transactions.
- **Business Information.** Information about products and services you provide (including inventory, pricing and other data) and other information you provide about you or your business (including appointment, staffing availability, employee, payroll and contact data).
- **Background Information.** To the extent permitted by applicable laws, we may obtain background check reports from public records of criminal convictions and arrest records. We may use your information, including your full name, government-issued identification number, and date of birth, to obtain such reports.
- **Other Information You Provide.** Information that you voluntarily provide to use, including your survey responses, participation in contests, suggestions for improvements, referrals, or any other actions performed.

6.1 How EmeSec Collects Information

EmeSec collects various types of personal information, including but not limited to:

- Information you provide us directly,
- Information we collect about your device(s) and your use of our Services, including through cookies, web beacons, and other internet technologies, and
- Information we obtain from third-party sources.

6.1.1 Personal Information You Provide Us Directly

EmeSec collects various types of information and content that you provide us directly. For example, during onboarding (employees, 1099s, and temp to perm) you will be requested to provide us with your name, telephone number, email address, postal address, and where applicable company or organization name. Employees hired directly will also be requested for additional information such as, Social Security Number, banking information, family member information for benefits, etc. We collect billing and payment information from 1099s. We also collect information that you provide us when you participate in our surveys, events, training, etc. In some circumstances, if you do not provide us with the requested information, we may be unable to fully complete your employment or contracting services.

To the extent that you disclose to us any personal information of another individual or yourself, we assume that you have obtained such individual's consent for the disclosure of such personal information as well as the processing of the same in accordance with the terms of this Policy. Examples include, but not limited to, HR enrollment, employment reference, shared resume, etc.

6.1.2 Information About Your Device(s) and Your Use of the Services

We collect information about how you use our device(s)/Network and, depending on the access permissions you are granted, other information, as specified below, from and about the computers, phones, and other devices where you install or access our information. We use standard internet technologies, such as cookies and web beacons, to collect information about your computer or device and your online activity, as explained in more detail in the section on cookies.

The information we may collect in this respect is:

- Your browser type and operating system;
- IP address and device identifiers;
- Your browsing behavior on our device(s)/Network;
- Websites you visit;
- Whether you have opened or forwarded e-mails;
- Your general or specific geographic location, such as through GPS, Bluetooth or WiFi signals to the extent permitted by the settings of your device(s).

If you use our internet connection, networks, telecommunications systems or information processing systems, your activity and any files or messages on those systems may also be monitored by EmeSec at any time, in accordance with applicable law, for purposes of an investigation or to ensure compliance with company policies.

6.1.3 Information from Third-Party Sources

We may obtain information about you from your company or organization, including when they may create or supplement your contract or staffing arrangements with EmeSec. You can review and amend this profile at any time. For further details, see: Accessing, Reviewing, and Updating your Personal Information.

We also receive information about you from publicly and commercially available sources and other third parties as permitted by law (i.e., JPAS, background screening, etc.). We may combine this information with other information we receive from or about you, where necessary.

We use the personal information that we collect as necessary and appropriate for the following purposes:

- To provide employment, 1099, or temp to perm contracting services. We use your personal information to verify your identity in connection with a transaction that you and/or your company or organization has initiated, to deliver notifications and other operational communications.
- To analyze how Users, navigate and use our device(s)/networks.
- To manage your performance.
- For audit and reporting purposes, to perform accounting and administrative tasks, and to enforce or manage legal claims.
- To deliver communications. For example, we may periodically contact you with offers and information about our products, services, features, and events; to send you newsletters or other information about topics that we believe may be of interest, to conduct online surveys, etc.
- For security and to protect, enforce, or defend legal rights, privacy, safety or property, whether our own or that of our employees or agents or others, and to enforce compliance with EmeSec policies and to comply with applicable law and government requests.
- Delivering a service/solution you have requested.
- Contact regarding satisfaction surveys/feedback.

7 SHARING OF PERSONAL INFORMATION

EmeSec may disclose your personal information in the following circumstances to the following parties:

- **Within EmeSec.** EmeSec may share personal information with those affiliates for the purposes mentioned above. These affiliates use your information in accordance with this policy.
- **Our Community**. This may include online and offline member communities, forums and networks that allow you to share and connect with others. We make this possible for EmeSec by creating a profile/email for new staff that contains your name. This profile is created and is accessible to other members within EmeSec. You can supplement your profile by adding additional information about yourself and your company or organization and by posting content and comments and you may be able to share your profile/email with a broader audience.
- **Service Providers**. We rely on third-party service providers to perform a variety of services on our behalf. For example, we may rely on service providers to host data and platforms, fulfill our product and service requests and answer your questions, send e-mails on our behalf, process payments or other services including, onboarding, payroll services, and analyze data to improve our products and services. Some of our hosted platforms may contain personal information, such as; name, phone number, email address, etc. that may be accessible to other employees of EmeSec (i.e., HRIS system and Applicant Tracking system).
- **Other Parties When Required by Law and as Necessary to Provide and Protect Our Services**. In some instances, we may disclose your personal information to law firms, auditors, consultants, the police, courts, tribunals and other law enforcement agencies.

- To provide you with the services you or your company or organization request, such as a disclosure of your information to a landlord in connection with a lease agreement, or to auditors or consultants;
- To comply with the law or respond to legal process or a request for cooperation by a government entity or law enforcement (which may include lawful access requests by U.S. and other courts, law enforcement and governmental authorities);
- To detect, suppress, and prevent fraud or verify and enforce compliance with the policies governing our Services; or
- Where permitted by law, to protect our rights, property, and safety or that of any of our respective affiliates, business partners, customers, staff members or employees and where otherwise required by law.

- **Other Parties in Connection with a Corporate Transaction**. We may disclose your personal information to an acquirer in the event we sell or transfer all or a portion of a business or assets to that third party, such as in connection with a merger or in the event of a bankruptcy reorganization or liquidation.
- **Third-Party Partners, With Your Consent**. We may request your consent to share personal information about you with third parties so that they may provide you with special offers, promotional materials, and other materials that may be of interest to you.
- **Other Parties at Your Company's or Organization's Direction**. In addition to the disclosures described in this Policy, we may share information about you with third parties when your company or organization requests such sharing. For example, we periodically may partner with third-parties to make products or services available to individual members or participating companies and organizations. If you or your company or organization requests to participate, we may share your information with the relevant third-party in connection with the requested product or service.
- **Aggregated and Non-Personal Information**. We also share with third-party's information in a manner that does not identify particular individuals, for example, information that has been aggregated with other records.

Our services may contain links to other sites that we do not own or operate. We may provide links to these third-party sites as a convenience. They are not intended as an endorsement of or referral to the linked services. The linked services are subject to their separate and independent privacy statements, notices, and terms, *which we recommend you read carefully*. The collection, use, and disclosure of your personal information will be subject to the privacy policies of the third-party and not this Policy.

8 HOW WE MAY USE YOUR INFORMATION

EmeSec may use information about you for a number of purposes including, but not limited to:

Providing, improving, and developing our services

- Determining whether our employment and/or services are available in your country;
- Processing or recording payment transactions or money transfers;
- Otherwise providing you with the products and features you choose to use;
- Providing, maintaining and improving our Services;
- Developing new products and services;

- Delivering the information and support you request, including technical notices, security alerts, and support and administrative messages including to resolve disputes, collect fees, and provide assistance for problems with our services;
- Improving, personalizing, and facilitating your use of our services; and
- Measuring, tracking, and analyzing trends and usage in connection with your use or the performance of our services.

Communicating with you

- Sending you information we think you may find useful or which you have requested from us about EmeSec; and
- Conducting surveys and collecting feedback.

Protecting our services and maintaining a trusted environment

- Protecting our employees, our customers', or your customers' rights or property, or the security or integrity of our Services;
- Enforcing our Terms of Agreements or other applicable documents or policies;
- Verifying your identity (i.e., through government-issued identification numbers);
- Complying with any applicable laws or regulations, or in response to lawful requests for information from the government or through legal process; and
- Fulfilling any other purpose disclosed to you in connection with our services.

Advertising and Marketing

- Marketing of our services;
- Communicating with you about opportunities, products, services, contests, promotions, discounts, incentives, surveys, and rewards offered by us and select partners;
- If we send you marketing emails, each email will contain instructions permitting you to "opt out" of receiving future marketing or other communications; and
- To learn about your choices regarding interest-based advertising and cross-device tracking, please see below.

Other Uses

- For any other purpose disclosed to you in connection with our services from time to time.

9 CHILDREN'S PRIVACY

EmeSec may collect personal information from children under the age of 13, through our third party HRIS for benefit purposes. If we learn that we have collected personal information on a child under the age of 13, for any other reason that for benefit purposes, EmeSec will deleted that data from your system. EmeSec encourages parents and guardians to go online with their children, to assist in making a child's online experience safer. Here are a few online tips to encourage online safety:

- Teach children never to give our personal information (such as name, address, phone number, school, and other information) unless supervised by a parent or responsible adult;
- Know the sites your children are visiting and which sites are appropriate; and

- Look for website privacy policies and know how your child's information is treated.

For more tips on protecting children's privacy online, please see the FTC website: http://ftc.gov/bcp/menus/consumer/tech/privacy.shtm

10 California Law

Residents of the State of California, under California Civil Code 1798.83, have the right to request from companies conducting business in California a list of all third parties to which the company has disclosed personal information during the preceding year for direct marketing purposes. Alternatively, the law provides that if the company has a privacy policy that gives either an opt-out or opt-in choice for use of your personal information by third parties (such as advertisers) for marketing purposes, the company may instead provide you with information on how to exercise your disclosure choice options.

11 Use of Cookies and Other Web Technologies

Like many websites, EmeSec may use automatic data collection tools, such as cookies, embedded weblinks, and web beacons. These tolls may collect certain standard information that your browser sends to our website such as your browser type and the address of the website from which you arrived at our website. They may also collect information about:

- Your Internet Protocol (IP) address. This is a number automatically assigned to your computer whenever you are surfing the web. It allows web servers to locate and identify your computer, which is a unique address, assigned to your PC by your internet service provider or information systems department on a TCP/IP network.
- Clickstream behavior. For example, the pages you view and the links you click.

These tools help make your visit to our website easier, more efficient, and more valuable by providing you with a customized experience and recognizing when you return.

Our website may include widgets, which are interactive mini-programs that run on our site to provide specific services from another company (such as news, opinions, music, and more). Personal information, such as your email address, may be collected through the widget to enable it to function properly. Information collected by this widget is governed by the privacy policy of the company that created it.

Some web browsers may give you the ability to enable a "do not track" feature that sends signals to the websites you visit, indicating that you do not want your online activities tracked. This is different than blocking or deleting cookies, as browsers with a "do not track" feature enabled may still accept cookies. There is currently no industry standard for how companies should respond to "do not track" signals, although one may develop in the future. We currently do not respond to "do not track" signals, if we do so in the future we will describe how in this Privacy Policy.

Each subscription email from us includes instructions on how you can unsubscribe from that mailing.

12 Data protection Risks

This policy helps to protect you and EmeSec from security risks, including:

- **Breaches of confidentiality**. Information being given out inappropriately
- **Failing to offer choice**. All individuals should be free to choose how the company uses data relating to them
- **Reputational damage**. EmeSec would suffer if hackers successfully gained access to sensitive data

13 General Staff Guidelines

The only people able to access data covered by the policy should be those who need it for their work. EmeSec provides training to all employees to help them understand their responsibilities when handling data. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- Passwords should be consistent with NIST and CUI guidelines, and they should never be shared,
- Personal data should not be disclosed to unauthorized people, either within EmeSec or externally, and
- Data should be regularly reviewed and updated; if it is found to be out of date or no longer required, it should be deleted or disposed of in accordance with the EmeSec Information Data and Document Lifecycle Management (IDDLM).

14 Data Storage and Retention

These guidelines describe how and where data should be safely stored. Questions about storing data safely can be directed to IT or the Data Protection Officer. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed:

- When not in use, paper and printouts should be kept in a drawer or filing cabinet;
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer; and
- Data printouts should be shredded and disposed of securely when no longer required or in accordance with the IDDLM.

When data is stored electronically, it must be protected from authorized access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared;
- If data is stored on removeable media (i.e., CD, DVD, Hard drive), these should be kept securely locked up while not in use;
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service;
- Servers containing personal data should be sited in a secure location;
- Data should be backed up frequently. Those backups should be tested regularly, in line with EmeSec's standard backup procedures;

- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones; and
- All servers and computers containing data should be protected by approved security software and a firewall.

We generally retain your information as long as reasonably necessary or to comply with applicable law. However, even after your separation from EmeSec, we can retain information about you and any transactions or services in which you may have participated for a period of time that is consistent with applicable law, applicable statute of limitations or as we believe is reasonably necessary to comply with applicable law, regulation, legal process, or governmental request, to detect or prevent fraud, to collect fees owed, to resolve disputes, to address problems with our services, to assist with investigations, to enforce our general terms or other applicable agreements or policies, or to take any other actions consistent with applicable law. When information is no longer necessary, it is to be shredded and/or disposed of securely when no longer required or in accordance with the EmeSec IDDLM.

15 Security

We take reasonable measures, including administrative, technical, and physical safeguards, to protect your information from loss, theft, misuse, and unauthorized access, disclosure, alteration, and destruction. Nevertheless, the internet is not a 100% secure environment, and *we cannot guarantee absolute security of the transmission or storage of your information*. We hold information about you both at our own premises and with the assistance of third-party service providers.

16 How to Contact Us

We value your opinion. Should you have any privacy related questions or comments related to EmeSec's Privacy Policy, please email us at privacy@emesec.net.

17 Updates to EmeSec Privacy Policy

We may update this Privacy Policy at any time, so *please review it frequently*. As rules on privacy evolve-other specifics may be added, check the HR Website for the most updated version. If we make significant changes to our Privacy Policy, we may also notify you by other means, such as sending an email, company newsletter, website notice, etc.