CONTENTS

1. Introduction

The Executive Office of the President (EOP), Office of Management and Budget (OMB)[1] Memorandum M-06-19, July, 12, 2006 identifies personally identifiable information as:

> ...the term Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

As such and since Monster Government Solutions (MGS) has the responsibility to protect our government clients' privacy information that has been entrusted to MGS, this policy will ensure that MGS complies with EOP OMB Memorandum M-06-15 and the Privacy Act of 1974 that requires:

> ...rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to this [Act] and the penalties for noncompliance", and "appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained."

Protection of privacy can be traced back in American History as far as the Fourth US Constitutional Amendment. Privacy protection issues have escalated as information technology and the Internet have made it easier to collect PII, leading to a profitable market in collecting and reselling PII. As a response to personal identity theft and privacy information threats, many web site privacy policies specifically address the collection of PII, and lawmakers have enacted a series of legislation to limit the distribution and accessibility of PII.

---

[1] Additional privacy protection guidance and regulations include E-Government Act of 2002, Office of Management and Budget (OMB) Circular No. A-11 and Exhibit 300.

This document addresses the various facets of collecting privacy information from general public in accordance with OMB M-03-22:

1. What information is to be collected;

2. Why the information is being collected;

3. The intended use of the agency of the information;

4. With whom the information will be shared;

5. What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

6. How the information will be secured; and

7. Whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the `Privacy Act').

MGS conducts PIAs on Information Technology (IT) systems that process, collect, store or dispose of privacy information. The PIA is a "checklist" that ensures electronic collection of individual information is:

- Evaluated for risk to privacy of individuals
- Designed to maintain, use and safeguard the information only as prescribed and is appropriate, and
- Ensure those mechanisms being used are adequate.

2. System Identification

SYSTEM NAME	Hiring Management System (HMS)
SYSTEM OWNER	Mark Madsen
OFFICE OF SYSTEM OWNER	Monster Government Solutions
INFORMATION ASSURANCE MANAGER	Mike Parker
PRIVACY OFFICER	Tony Parker
SYSTEM SECURITY CATEGORIZATION	Moderate

The Hiring Management system (HMS) is a Major Application provided to the customers of Monster Government Solutions (MGS) as a Human Resources (HR) management and staffing solution. This application is a Web Based system that customers use via the Internet as a tool for electronic automation of staffing and HR management related functions. Functions include creating and managing vacancies, notifying potential applicants of those vacancies via the Internet, collecting and processing applicant data, and ranking applicants' qualifications based on such data. Information stored and processed by the Hiring Management application include vacancy data such as job descriptions, questions, and criteria; as well as applicant data such as resumes, contact information, and social security numbers.

HMS relies on a computer network, including several hardware and software components to function. All data used by Hiring Management is stored in electronic database format on database servers. A separate database file is used for each customer/organization. This database is then accessed and processed by software components, each of which has their own purpose. The software components are what make up HMS.

3. The System and the Information within the System

3.1 What information is being collected

Information that is collected and stored by HMS includes the following:

- Name
- Address
- Phone Number
- Email Address
- Social Security Number (SSN)
- Resumes
- Job Descriptions

3.2 Why the information is being collected

The information is collected in support of the MGS HMS application mission. This includes identifying an applicant's education and work skills to match them to a fitting Federal job and to notify applicants of vacancies via the Internet.

3.3 The intended use of the information

The data that is collected by HMS is owned by the Federal customer and used in support of its functions as an electronic automation solution for HR management. The federal client is responsible for adhering to their privacy statement and informing users of their information use.

3.4 With whom the information will be shared

MGS does not disclose applicants' personal information in its customers' HMS systems to third parties, their combined personal and demographic information, or information about use of MGS (such as the areas visited or services accessed), with the following exceptions:

- MGS discloses information to third parties at the applicant's request for such disclosure. Such consent, indicating that the customer would like information transmitted to a third party would be part of a change authorization.
- MGS discloses information to companies and individuals we employ to perform functions on our behalf. Examples include hosting our Web servers, analyzing data, and providing customer service. These companies and individuals will have access to customers' applicants' personal information as necessary to perform their functions, but they may not share that information with any other third party.

- MGS discloses information if legally required to do so, if requested to do so by a governmental entity or if it believes in good faith that such action is necessary to: (a) conform to legal requirements or comply with legal process; (b) protect its rights or property or its affiliated companies; (c) prevent a crime or protect national security; or (d) protect the personal safety of users or the public.
- MGS discloses and transfers information to a third party who acquires all or a substantial portion of its business, whether such acquisition is by way of merger, consolidation or purchase of all or a substantial portion of its assets. In addition, in the event MGS becomes the subject of a bankruptcy proceeding, whether voluntary or involuntary, MGS or its trustee in bankruptcy may sell, license or otherwise dispose of such information in a transaction approved by the bankruptcy court. Customers will be notified of sale of all or a substantial portion of MGS' business to a third party via email or through a prominent notice posted on the Monster Sites.

3.5 Notification of Consent

MGS Hiring Management' Privacy Statement is posted on the HMS website. . At the time of registration, consent may be given, indicating that the customer would like to receive information about new job postings. Links to customers' privacy statements are available upon request.

3.6 Reporting

The HMS is a Major Application provided to the customers of Monster Government Solutions (MGS) as an Human Resources (HR) management and staffing solution. This application is a Web Based system that customers use via the Internet as a tool for electronic automation of staffing and HR management related functions. Report generation functions include creating and managing vacancies, notification to potential applicants, collecting and processing applicant data, and ranking applicants' qualifications based on such data. Vacancy data such as job descriptions, questions, and criteria; as well as applicant data such as resumes, contact information, and social security numbers is also available. (Section 3.1 though 3.4 above)

Access to HMS database is restricted to authorized users by user name, password, and IP address. See section 3.8 for details.

3.7 Retention Periods of This Data

HMS maintains data indefinitely, at data end-of-life or an interval specified by the customer data is transferred from the system onto CD and passed to the customer for final disposal. Format and security of the data on the CD are at the direction of the HMS customer.

3.8 How the information will be secured

All of the HMS components are currently located in a secure cage in an IBX facility, where access is strictly limited to authorized personnel. User records are maintained indefinitely and secured within the HMS database. Records that are no longer valid are disabled.

Access to HMS is conducted over an AES SSL-encrypted connection via the Internet and via a AES VPN tunnel from the MGS office for administration. Other types of controls and limitations are also in effect. Remote access to the HMS is not permitted except for a limited number of MGS employees for administrator purposes.

HMS operates behind a firewall, which only allows access from the Internet via HTTPS. HMS is also restricted by an Access List and is not open to the public.

The system has anti-virus protection that is updated on a daily basis. System logs are reviewed on a weekly basis to check for anomalies such as hacking attempts.