SIRVA SUPPLIER CODE OF CONDUCT

A COMMITMENT TO INTEGRITY

Last Updated: March 2023

TABLE OF CONTENTS

INTRODUCTION: A MESSAGE FROM SIRVA SUPPLY CHAIN MANAGEMENT

Sirva and its affiliated entities (collectively referred to herein as "Sirva") is committed to operating with business and ethical integrity and we expect the same from our suppliers and partners. We want to ensure that working conditions in our supply chain are safe, that workers are treated with respect and dignity, and that their environment is both legally compliant as well as conducive to success.

To ensure our expectations and provide guidance for meeting these shared standards, Sirva has developed this Supplier Code of Conduct (the "Supplier Code"). This Supplier Code applies to all Sirva suppliers of products or services, including but not limited to consulting firms, independent contractors, staffing agencies, or agency temps, regardless of title or the product or service that they provide. These groups are collectively referred to herein as "Suppliers." Sirva expects each Supplier to uphold this Supplier Code and conform to its standards in all jurisdictions in which the Supplier conducts business on behalf of Sirva and its Clients. Further, prior to utilizing any subcontractor, consultant, independent contractor[1] or any other third party to provide services on behalf of Sirva or its Clients ("Subcontractor"), and at reasonable periodic intervals thereafter, Supplier shall perform appropriate due diligence and/or auditing to ensure that the Subcontractor complies with the requirements set forth herein.

Suppliers are expected to identify and correct any activities that fall below the standards set forth herein. Suppliers shall immediately report any breach of the Supplier Code by Supplier or its Subcontractor, to Sirva. Suppliers will cooperate with Sirva in the investigation of any violation of the Supplier Code and shall employ the appropriate corrective action for such violation. Sirva reserves the right to terminate the business relationship should, in Sirva's sole discretion, a violation be incapable of correction.

Sirva monitors Suppliers via annual review of security reports (where available) and factor model risk questionnaires, through which it evaluates and ranks each supplier's overall risk level. Sirva reserves the right to conduct further audits and monitoring of Suppliers at its discretion to ensure that all Suppliers comply with the principles set forth herein. As a supplement to this policy, suppliers are required to comply with the Responsible Business Alliance Code of Conduct. The Responsible Business Alliance Code of Conduct can be found here: http://www.responsiblebusiness.org/code-of-conduct/

We look forward to working with you and your organization to bring the best in service to our clients and customers. As part of our commitment to transparency and a quality business relationship with Suppliers, we encourage open communication and discussion of any of the topics addressed in this Supplier Code. If you have any questions about this Supplier Code or Sirva's overall process, please reach out to your Sirva contact, a member of the Sirva Supply Chain department or email us directly at suppliercomments@sirva.com.

John O'Connell

John O'Connell
EVP, Global Account Management and Supply Chain

1 For real estate brokerage companies, these requirements apply equally to sales agents, brokers, and other licensees associated with your company.

SUPPLIER CODE OF BUSINESS CONDUCT AND ETHICS

1. Confidential Information and Protection of Personal Data

A. Protect Sirva Confidential Information at all Times.

You must always protect Sirva Confidential Information. Your obligation to protect this information continues if your relationship with Sirva is terminated for any reason. Internal discussions regarding Sirva and Sirva Confidential Information should be limited to those who "need to know" the information. Additionally, be careful not to discuss Sirva Confidential Information in public places such as elevators, restaurants, and public transportation, or when using your phone or email outside of the office. You should also be careful not to leave Sirva Confidential Information in unattended conference rooms or in public places where others can access it. For purposes of this Supplier Code, "Sirva Confidential Information" means, without limitation, information in any format pertaining to Sirva's pricing, financial data, business strategies, contracts, technology, network architecture, branding, trade secrets, the policies contained herein, and any information in connection with Sirva's clients, assignees, and transferees (such as Personal Data, as defined below).

B. Comply with Data Protection Laws.

You may be granted access to Personal Data d to perform your services. Personal Data should always be handled and processed in accordance with contractual, legal, regulatory and obligations, such as those set forth under the *General Data Protection Regulation* ("GDPR") and should only be retained by you for as long as it is necessary to satisfy a legitimate business purpose or to satisfy a legal or regulatory obligation. You must take all reasonable steps to ensure that Personal Data is accessed only by those individuals at your company who have a need to know this information in order to carry out their duties. In addition, if it is necessary to disclose Personal Data to a third party (e.g., so that a third party may provide services to the customer or client) then you must ensure that the third party is subject to a confidentiality obligation. For purposes of this Supplier Code, "Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

C. Adhere to Sirva's Baseline Security Requirements

Any person or entity, also referred to as "data recipient" that has access to, processes, transmits, or stores Confidential Information or has access to Sirva's systems, shall adhere to Sirva's Baseline Security Requirements, attached as Exhibit A.

D. Honor Sirva's Intellectual Property Rights

Sirva expects Suppliers to honor intellectual property rights. Suppliers are not permitted to obtain, distribute, or use unlicensed material without the authorization of the creator or license-holder. Your Sirva contact can answer any questions that you may have about the proper use of materials subject to intellectual property restrictions.

2. Accuracy of Books and Records and Public Disclosures

A. Ensure That Your Books and Records are Complete and Accurate, and That all Business Transactions are Properly Authorized.

The books and records of your company must reflect all its transactions in order to permit the preparation of accurate financial statements. You must never conceal information from (i) an external auditor; (ii) internal auditor; or (iii) an audit committee. In addition, it is unlawful for any person to fraudulently influence, coerce, manipulate or mislead an auditor.

B. Ensure Accurate and Truthful Public Disclosure.

You must ensure that public disclosures of information are made honestly and accurately. Employees of your company must be aware of and report any of the following: (a) fraud or deliberate errors in the preparation, maintenance, evaluation, review or audit of any financial statement or financial record; (b) deficiencies in, or noncompliance with, internal accounting controls; (c) misrepresentations or false statements in any public disclosure document, such as annual and quarterly reports, prospectuses, information/proxy circulars and press releases; or (d) deviations from full and fair reporting of the company's financial condition.

Additionally, each person who is in a financial reporting oversight role, and their immediate family members, are prohibited from obtaining any tax or other services from the external auditor, irrespective of whether the company or such person pays for the services.

3. Conflicts of Interest and Personal Behavior

A "conflict of interest" for this purpose relates to a person's private interest interfering, or even appearing to interfere, with the best interests of the company. Employees should always place the company's interest in any business matter ahead of any personal interest. Remember that the company's interest includes the company's obligations to its clients and customers.

If you or your employees are pursuing personal, political, not-for-profit activities, be mindful that your participation in such activities must not prevent you from adequately performing your duties for Sirva. In addition, ensure that when you are involved in these activities you are not seen to be speaking or acting on behalf of the company or Sirva without express authority.

4. Social Responsibility and Respect

A. Ensure a Tolerant Work Environment Free from Discrimination, Violence and Harassment.

Your company should have a policy in place that strictly prohibits discrimination and harassment, retaliation, or any other form of abuse. Employment-related decisions should be made on the basis of a worker's knowledge and skill, without regard to race, color, religion, national origin, age, medical condition or disability, marital status, pregnancy, or sexual orientation.

B. Ensure the Health and Safety of Staff.

Your company must comply with all occupational, health and safety laws and must not engage in illegal or dangerous behavior.

C. *Human Rights*

Your company must ensure to strictly follow all laws related to child labor, forced labor, employee working hours, payment of employees (including minimum wage laws and overtime) and the working environment.[2] Child labor, slavery, and human trafficking are not tolerated under any circumstances.

5. Compliance With Laws, Rules, Regulations and Policies

A. *Your Company and Employees are Responsible for Understanding and Complying with all Applicable Laws, Rules and Regulations.*

You are expected to pro-actively identify, monitor, and comply with all applicable laws, rules, regulations and policies affecting your services to Sirva.

B. *You Must Prevent the Use of Your Operations for Money Laundering or Any Activity that Facilitates Money Laundering, the Financing of Terrorism, or Other Criminal Activities.*

Jurisdictions may publish lists of individuals and organizations that the company is prohibited from accepting funds from or distributing funds to under applicable anti-money laundering laws. You are expected to use reasonable care to verify that counterparties are not owned or controlled by, or acting on behalf of, sanctioned governments, groups, individuals or others.

C. *Compliance with Anti-Bribery and Corruption Laws*[3]

i. What do Anti-Bribery Laws Prohibit?

The Foreign Corrupt Practices Act ("FCPA"), the UK Bribery Act and other anti-bribery laws make it unlawful to bribe a foreign official to gain an "improper business advantage." An improper business advantage may involve efforts to obtain or retain business, as in the awarding of a government contract, but also can involve regulatory actions such as licensing or approvals. Sirva has a *Zero-Tolerance Policy* for bribes.

A "foreign official" is any person who exercises governmental authority. A foreign official includes elected or appointed persons who hold legislative, administrative or judicial positions such as politicians, bureaucrats, civil servants, and judges. Officials and employees of government-owned or controlled enterprises also are covered, as are private citizens who act in an official governmental capacity. Foreign official status often will be apparent, but not always. In some instances, individuals may not consider themselves officials or be treated as such by their own governments but nevertheless exercise authority that would make them a "foreign official" for purposes of anti-bribery laws. There is increased sensitivity and scrutiny of dealings with public officials because this has traditionally been an area where bribery activity is more likely to occur. Be aware of these risks in your dealings and interactions with public officials and consider how your actions may be viewed.

---

[2] References

- The United Nations Universal Declaration of Human Rights.
- The Conventions of the International Labour Organisation.
- The United Nations Convention on the Rights of the Child and the UK Modern Slavery Act of 2015.

[3] For moving agents, SIRVA is committed to FIDI's Anti-Bribery and Corruption Charter https://www.fidi.org/about-fidi/fidis-vision-mission/anti-bribery-and-anti-corruption-charter

ii. What is a Bribe?

A bribe is anything of value that is offered, promised, given or received to improperly influence a decision or to gain an improper or unfair advantage in promoting, enhancing, obtaining or retaining business. Bribery includes but is not limited to:

- Gifts, travel, and hospitality;
- Political contributions;
- Charitable donations (note, Charitable donations made by individuals on their own behalf should have no relationship to company business and must comply with local laws and regulations);
- Employment opportunities or internships;
- Procurement and service contracts;
- Phony jobs or "consulting" relationships;
- Excessive discounts or rebates;
- Non-arm's length loans, forgiveness of debt or other transactions; and/or
- Facilitation payments or small payments made to secure or speed up routine actions or otherwise induce public officials or other third parties to perform routine functions they are otherwise obligated to perform, such as issuing permits, approving immigration documents, or releasing goods held in customs, even if the facilitation payment is permitted under local law.

iii. Gifts and Entertainment

Gifts and entertainment (e.g. merchandise, event tickets, concerts, rounds of golf) given to or received from persons who have a business relationship with the company are generally acceptable (unless the Supplier is participating in an RFP or other review), if the gift is modest in value, infrequent, appropriate to the business relationship, does not create an appearance of impropriety, and in the case of an event, if a representative from the sponsoring organization (i.e., the party paying for the entertainment) is present at the event. No cash payments should be given or received. In addition, gifts cannot be given to or received from public officials and special attention should be paid to the laws regarding entertainment in your jurisdiction as many have laws restricting entertainment given to public officials or their close relatives.

iv. Record Keeping

In addition to prohibiting bribery, some anti-bribery legislation and other laws expressly require accurate and complete record-keeping and the establishment and maintenance of an adequate system of internal controls. One purpose of these provisions is to prevent companies from concealing bribes and to discourage fraudulent accounting practices.

All transactions must be recorded completely, accurately and with sufficient detail so that the purpose and amount of any such payment is clear. No undisclosed or unrecorded funds or assets of your company should be established for any purpose. False, misleading, or artificial entries should never be made in the books and records of your company for any reason.

D. If You are a Sirva Supplier Working on Federal Government Agency Assignments, You Must Comply with all Federal Regulations Listed in Exhibit B.

As a prime contractor to several federal government agencies, Sirva is required to incorporate ("flow down") certain provisions of its prime contract into its agreements with subcontractors and vendors. Accordingly, the provisions identified in Exhibit B shall expressly flow down to all contracts, agreements, solicitations, work orders, purchase orders, or other requests for service between Sirva and the Sirva Supplier when performed in support of US federal government agency relocation assignments. Most of the contract provisions are embodied within the Federal Acquisition Regulations ("FAR") or agency specific regulations, the full text of which are available at www.acquisition.gov. Descriptions of the provisions are found in Exhibit B and are provided for convenience only and the Sirva Supplier should consult the actual provision for applicability and specific requirements.

E. If You are a Sirva Supplier Working on Honeywell FM&T Assignments, You Must Comply with All Federal Regulations Listed in Exhibit C.

Honeywell FM&T is a Management and Operating (M&O) Contractor for the U.S. Department of Energy (DOE). As such, Honeywell is required to flow down various provisions to its subcontractors, including Sirva, and Sirva is required to flow down these provisions to Sirva Suppliers who perform work on Honeywell FM&T assignments. The Honeywell flow down provisions are listed in Exhibit C. Most of the contract provisions are embodied within the FAR, and the full text can be found at www.acquisition.gov. Sirva Suppliers should consult the actual provision for applicability and specific requirements.

D. Compliance with Anti-Trust Laws

Sirva is committed to competing in a fair and vigorous manner, in compliance with all applicable antitrust and competition laws. Antitrust laws protect consumers by prohibiting anticompetitive conduct that can restrict free competition. In accordance with these laws and regulations, Suppliers must never agree, either directly or indirectly, with competitors: (1) to set prices or other terms related to your products; (2) to allocate customers, advertisers, territories, or product markets; or (3) not to deal with a particular company (called a "group boycott").[4]

6. Corporate Initiatives

From time to time, Sirva may engage in initiatives to improve the public well-being or general welfare such as corporate sustainability initiatives, education advancement initiatives, equal employment initiatives or consumer protection initiatives. As a condition of this relationship, Supplier will be expected to support such initiatives and projects upon request of Sirva. For such initiatives or projects Sirva will work with supplier to establish goals, performance expectations and reporting requirements.

7. Environmental, Social and Governance

Sirva recognizes the impact our global business can have on the environment and is committed to ensuring we leave a positive mark on the communities and world in which we live and work. We strive to implement environmentally friendly and sustainable initiatives across all segments of our operations. We are committed to achieving a model of sustainability excellence that carries across all channels and all locations

[4] For moving agents, SIRVA is committed to FIDI's Anti-Trust Charter https://www.fidi.org/about-fidi/fidis-vision-mission/fidi-anti-trust-charter-0

of our business. In extension, our suppliers are expected to conduct business with a goal toward improving environmental conditions and comply with all applicable environmental laws and regulations.

The environmental sustainability covers energy consumption, greenhouse gas emissions and water and waste management. In all these areas, the basic criteria which Sirva Suppliers need to adhere to are:

- Comply with all environmental legislation applicable in their location and industry
- Have an environmental policy that outlines efforts and goals in the above areas
- Operate at the best efficiency and minimize waste and CO2e emissions
- Train employees on best practices and regulations
- Respond to Sirva annual surveys within deadline
- Follow Sirva evolving guidelines and implement new steps when requested (if the new requests are not possible to deliver, inform Sirva as soon as possible why this is not possible and if there are any other paths to achieve similar outcome)
- Report their environmental activities to Sirva on an annual basis

8. Communication/Emergencies

Emergency situations and events are to be identified and assessed, and their impact minimized by implementing emergency plans and response procedures. An emergency may include a natural or unnatural disaster such as a storm, flood, earthquake, landslide, an act of civil unrest or any other situation that may put a shipper, transferee, assignee, their family or property in danger, or may cause a serious inconvenience or delay in the process of a shipment or relocation.

The following is a high-level process that should be followed in an emergency:

1. Identify and mitigate problems before a crisis.
2. If an emergency happens, follow emergency preparedness protocols.
3. Anticipate the consequences of the emergency.
4. React to the emergency appropriately and quickly.
5. Recover from the emergency.

If a Sirva shipper, transferee or assignee is in any type of danger, or you are aware of an actual or potential emergency, call your Sirva Supply Chain manager or consultant directly.

9. Sirva Ethics Reporting Hotline

Sirva has teamed with Safecall, an independent third-party reporting hotline. All calls are treated confidentially by Safecall and you will remain anonymous if you wish. Report online at: www.safecall.co.uk/report

COUNTRY	NUMBER
Australia	800 312 928
Brazil	0 800 892 1750
Canada	877 599 8073
China	1 0 800 744 0605 1 0 800 440 0682
Finland	999 800 7233 2255 990 800 7233 2255
Germany	00 800 7233 2255
India	000 800 4401 256

COUNTRY	NUMBER
Netherlands	00 800 7233 2255
New Zealand	00 800 7233 2255
Singapore	800 448 1773
S. Africa	0 800 990 243
UAE	8000 441 3376
UK	0800 915 1571
USA	866 901 3295

For a list of additional toll-free numbers, please visit: www.safecall.co.uk/freephone

EXHIBIT A: BASELINE SECURITY REQUIREMENTS

If Supplier has access to Sirva's systems or has access to Personally Identifiable Information (PII), in the course of providing Services to Sirva and its Clients, Supplier represents and warrants that it shall use commercially reasonable efforts to maintain the stated control requirements below, and will document those efforts. Any deviation from these controls will require written approval from the Sirva CISO. This documentation may be reviewed by Auditors to assess the merit of the rationale. Supplier further represents and warrants that Supplier's systems and systems media that store, process transmit Sirva information or otherwise interact with Sirva shall be protected against unauthorized access, acquisition, use, theft, loss, disclosure, manipulation, damage or interference to the security, confidentiality or integrity of such information. This representation, together with these Information Security Requirements, do not limit Supplier's obligations or liability for any breach, regardless of efforts used by Supplier, under the Agreement or applicable law and do not limit the scope of an audit by Sirva.

OBJECTIVE	REQUIREMENTS
1. Ensure effective management of information and technology assets and ensure that assets are accounted for.	1. Establish and maintain an inventory of information technology assets. The listing should include: a. All applications, software, databases, network and network security infrastructure devices, access points, circuits and other hardware type assets. b. All User IDs for users of the systems. c. Physical and logical locations and diagrams. d. A Data Loss Prevention (DLP) solution designed to detect and prevent unauthorized use, removal, or transmission of confidential information at the user endpoint.
2. Ensure that cryptographic controls are strong enough to protect Confidential Information.	1. Encrypt all Confidential Information (whether in electronic, digital, optical, magnetic or other similar format or media), including authentication credentials, while in transit over any network or stored on any device with a minimum of 128-bit encryption. 2. A secure key management process will be employed and comply with local restrictions and regulations.
3. Ensure that the operating system(s) is (are) logically protected from unauthorized access and transactions.	1. Document and implement standard global security settings or parameters as appropriate to each operating system in use. 2. Operating systems should be updated to the latest security release.
4. Discourage inappropriate usage and unauthorized access to Confidential Information by providing a basis for action against anyone disregarding the banner's message.	1. Supplier will provide a visual banner on workstations and internal networking devices to warn against unauthorized and inappropriate access, including displaying the banner to users prior to system login and with the banner remaining on the screen until action is taken to acknowledge the message. 2. Supplier will display a similar security acknowledgement banner to users accessing publicly accessible interfaces that provide access to internal systems, including any remote access VPN.
5. Ensure that network and security infrastructure are configured to prevent unauthorized access to the device(s) and are deployed in a manner which will not place Confidential Information or assets at risk.	1. Supplier should have policies and standards that prevent unauthorized infrastructure devices to be added to its network without formal approval. 2. Supplier will deploy all network security monitoring devices, including network intrusion detection sensors, in such a manner that a failure of a particular device does not cause an interruption in the monitoring functionality that the device provides. 3. Supplier will ensure that security gateways fail "closed" so that no unauthorized traffic passes through the security gateway even if the security gateway cannot communicate with an associated management station. 4. Supplier will segregate networks and control requirements for access between networks to ensure appropriate authorized and controlled communications (*e.g.*, create domain classifications). 5. Supplier will disable unused network interfaces and physical ports on network and security infrastructure devices.

OBJECTIVE	REQUIREMENTS
	6. Supplier will configure all network and security infrastructure devices to prevent unauthorized access (whether in-band or out-of-band) to management, administrative, or monitoring functions. 7. Supplier should define a quality assurance process to minimize the risk of errors or unauthorized functionality being configured into security gateways. 8. Supplier will set internal clocks on all network and security infrastructure devices accurately and synchronize them, directly or indirectly, to an official time source. 9. Supplier will configure network and security infrastructure devices with approved and authorized baselines. 10. Supplier will deploy all authentication, authorization, and audit services used to control and record access to network and security devices such that a failure of a particular instance of the service does not cause an interruption to, or reduce the reliability of, authentication, authorization and audit functionality.
6. Prevent activation of unnecessary services.	1. Supplier will review services (*e.g.*, SNMP, DNS, DHCP, WINS, HTTP, FTP, SMTP) and consider them for deactivation.
7. Ensure that all network and telecommunication connections are identified and regularly assessed for vulnerabilities.	1. All devices attached to the network, including network and security infrastructure devices and telecommunication connections will be assessed no less than every 90 days
8. Ensure that remote access users use an authorized and approved solution for remote access.	1. Supplier will subject all remote access users and devices to appropriate authorization and authentication using an appropriate, approved two-factor authentication mechanism to reliably establish a user's identity, and to ensure full accountability for all actions performed under that identity. 2. Supplier will encrypt all remote access via any shared network.
9. Ensure that file transfer solutions are capable of terminating, validating, and verifying the integrity of the data.	1. Supplier will terminate communications with file transfer devices that send or receive data directly with third parties before passing the file along to other internal devices. 2. Supplier will only use file transfer solutions that are capable of encrypting communications, both data and command, and that provide confirmation of delivery at the final destination.
10. Ensure that all network and security infrastructure devices are monitored to verify compliance with approved baselines, and that event-monitoring is near real time in frequency.	1. Intrusion Detection/Protection (IDS) devices should be placed at all entry and exit points of the security gateways and will have visibility of all traffic within the security domain. 2. Compliance monitoring tools will be actively running on or against the device or appliance to inspect the configuration of the operating system. 3. All network devices will be running or subjected to an event-monitoring solution.
11. Ensure a log or audit trail of all management activity, including configuration changes, will be maintained. Ensure that logs of successful and unsuccessful connection attempts will be available.	1. The audit trails will be reviewed and all exceptions investigated and documented in a timely manner. 2. Audit trails will be preserved at least 90 days and be retrievable for a period of at least one year. 3. All infrastructure devices will perform extensive documented logging.
12. Identify and respond to suspicious connection activity.	1. Event alerts will be collected and stored and accessible for review and subsequent response. 2. Firewall logging will be at each tier and be protected from unauthorized access, modification, destruction and activation/deactivation. 3. Audit logs will be generated to account for the following events: all user logins, Admin logins via privilege management applications such as “su” and “sudo”, policy and configuration changes, and user account creation and deletion. 4. Firewall policy logs will capture: Source and destination ports and IP addresses, Date and Time (including time zone), Session termination, Action – permitted or denied, ID of firewall enforcement device, firewall

OBJECTIVE	REQUIREMENTS
	interface, reference to a specific firewall policy or rule responsible for the action.
13. Ensure that configurable systems log all significant security related events.	1. Network devices (*e.g.,* routers and switches) will be configured with logging and auditing features. 2. Auditing will be enabled for network, system, and connection sessions. 3. Network protocol traffic activities, user system activity, system management, and security management activities should be logged. 4. Logs will be reviewed in a periodic and timely manner and protected from unauthorized access, modification, destruction and activation/deactivation. 5. System storage structures, creation, alteration, and deletion of any database will be audited.
14. Log entries will provide sufficient information to facilitate investigation and potential prosecution or civil remedy pursuant to security breaches.	1. The following will be audited: a. Enabling and disabling of audit functionality. b. Any updates and deletion of audit information. 2. Minimum information to be included in audit trails: a. The User ID associated with the audit record. b. The change that was made, including the command that was issued. c. A timestamp (including date and time zone) of when the command was issued. d. Whether the command was successfully executed or not. 3. Minimum information to be included in infrastructure device logs: a. Details about the destination device/service that is being accessed. b. Details about the source device that initiated the connection. c. Authentication/authorization details if applicable. d. Timestamp. 4. Timestamps will be configured to show time zone and milliseconds to permit the most accurate time stamp to be generated. 5. Audit trails will not be stored solely on the device that created the records.
15. Protect corporate assets and Confidential Information by standardizing on a proven firewall technology that is scalable, stateful, application-aware, and provides packet-filtering performance.	1. Firewall strategies will be multi-tiered, with well-defined functionality for logging, management, and enforcement in each respective layer. 2. Firewalls will be capable of stateful packet inspection of OSI layers 3 (Network) and 4 (Transport). 3. A resilient firewall infrastructure solution will be used to reduce or eliminate network and operational downtime due to a single point of failure. 4. Firewalls will: a. be protected from unnecessary access; b. be set to “deny all” access unless specifically allowed; and c. not provide for any unnecessary functions or services. 5. Firewall rule sets and configurations will be recertified on a regular basis. 6. Firewall rule sets and strategy should be documented to facilitate recertification and allow consistent enforcement of rules. 7. Administration of firewall devices, policy, and configuration changes should be limited to authorized Users and based on necessary job responsibilities.
16. Ensure the protection of network router devices by controlling their access.	1. Access to routers/switches will be controlled from both a physical and network perspective. 2. Roles and responsibilities of Users accessing network devices will be clearly defined. Appropriate permissions will be granted for logging into devices. 3. Production routers/switches will be in secure facilities and communications rooms.
17. Provide strong authentication and non-repudiation for users logging into routers/switches.	1. All users that are involved with router maintenance will be centrally authenticated and have individual User IDs.
18. Provide a secure infrastructure for management servers, to minimize the	1. A separate network should be created for managing network devices. 2. All management traffic will pass through a firewall with filtering and logging enabled.

OBJECTIVE	REQUIREMENTS
threat of unauthorized access to network devices.	3. Configuration baselines and procedures will be established and documented to verify and certify devices before placement into production environments. 4. Network device configuration files will be regularly reviewed to ensure compliance with security Standards, thereby minimizing risk of unauthorized access. 5. All routers and switch rule sets will be reviewed once every quarter.
19. Ensure that information to be archived is moved to an off-premises location.	1. Backup data will be treated as the original data and have the same reading/copying rights and data protection.
20. Prevent unauthorized access to web services.	1. All inbound communications to devices will be restricted to the assigned public IP address of the application. 2. Services with source address restrictions will not run on the same server as a device that has services open to the Internet. 3. All external and network traffic originating from any given security domain (or tier) will terminate in the next security domain (or tier) before being passed on.
21. Ensure that where authentication is required it is performed in an internal device.	1. Where no authentication is required, an application will ensure that user sessions are contained within a given security domain. 2. Generic proxy usage that forwards traffic beyond the internal network will not be used. 3. Payload will be scanned for malicious code prior to relaying the file into the network.
22. Ensure that application development procedures include appropriate controls to prevent malicious code and unauthorized access.	1. All client-side data should be inspected (data type, size, and composition), including URL parameters, cookies, and hidden fields before passing to command shells, interpreters, or external programs. 2. Scripts will ensure buffer overflow conditions cannot be exploited. 3. Personal information (such as account number, National or social security number, birth date) should not be fully displayed on a screen.
23. Ensure that no one person with information security-related responsibilities can obtain control of information resources, such that the one person could successfully commit fraudulent or otherwise unauthorized functions without collusion with others.	1. Databases will have a set of logical roles to perform key responsibilities. 2. Network services to databases will be protected using authentication controls. 3. Database products will maintain transactional integrity of the database objects.
24. Prevent unauthorized access by implementing controls to authenticate all users to Sirva systems prior to gaining access.	A. <u>User ID Management</u> 1. User access procedures will be documented that identify user roles and their privileges, how access is granted, changed and terminated, and logging/monitoring requirements and mechanisms. 2. User access should be recertified at least annually. 3. Supplier will assign unique user IDs to each person with access to Sirva environments. 4. User IDs should be documented such that incidents can be traced to a specific individual. 5. Once a user ID is assigned to a user, the user ID may not be reassigned. 6. User IDs will be disabled after 90 days, and purged after 180 days, of logon inactivity. 7. User IDs supplied with externally procured software should be changed, documented, and controlled. 8. "Least privilege" access rights should be deployed. 9. A maximum login period should be established which disconnects remote users upon expiration. 10. Administrator accounts should be renamed (or disabled), and responsibilities assigned to individual IDs. 11. Access provisioning processes should require proper signoff, employ appropriate segregation of duties, and be documented. B. <u>Password Controls</u> 1. Passwords should incorporate the following characteristics:

OBJECTIVE	REQUIREMENTS
	a. Be at least 8 characters for single factor authentication systems, or be at least 4 characters for both factors in two-factor authentication systems. b. Not be easily guessed words or be the same initial password assigned to multiple IDs. c. Not be the user's name, user ID, national identifier. Social Security Number, date of birth, telephone number, mother's maiden name, etc. d. Be alphanumeric; not contain all letters or all numbers. e. Maintain its password file in a one-way encrypted state (*e.g.*, non-reversible), with no user having the capability of viewing actual passwords. 2. Password confirmation or resets will force re-authentication upon the first logon. 3. Application accounts that cannot be required to expire passwords will be documented. C. <u>Authentication Controls</u> 1. Error messaging will not reveal authentication information back to a user, a server name, or addressing information. 2. Logon credentials will not display on screen. 3. Logon credentials will validate only upon completion of all logon credentials. 4. All logon attempts will be limited to a maximum of five. 5. A single User ID will not be permitted to logon to a system or application from more than one physical location at a time, unless the operating platform (*e.g.*, the Internet) does not support this control or specifically authorized based on documented business need. 6. Authentication credentials that are stored to facilitate a secure logon process will be protected from unauthorized access. 7. Users will change their authentication credentials at least once every 90-day period. 8. Change to authentication credentials will not be the same as the previous five authentication credentials that were used. 9. All developer access will follow the same controls and standards as any others who are granted access. 10. Workstations and user accounts should invoke validation of the user credentials when inactive for longer than 15 minutes. 11. Authentication reset procedures will be documented and implemented.
25. Ensure that no individual be allowed to accumulate, retain, or be granted information, responsibilities, oversight, knowledge, functionality, or access which would enable or allow the commission of fraudulent, criminal, or otherwise unauthorized functions by that individual acting alone.	1. A separation of duties will be enforced among individuals who authorize access, individuals who enable access, and individuals who certify that access. 2. A separation of duties will be enforced among: a. users who request changes, b. project managers/application developers, c. those that create changes, d. user acceptance testers who test changes, e. production processing operations managers, and f. those who elevate changes into production. 3. Specifically, application developers will not have on-going update access to production environments.
26. Ensure all changes to production environments, including the introduction of or changes to technology infrastructure products, are controlled through a standard change promotion process.	1. Change control process documentation should include key deliverables, roles, responsibilities, and audit trail documentation. 2. Scheduled changes will be tested prior to production. 3. Changes should be tracked and approved according to that documentation prior to implementation. 4. Changes should be validated to ensure only approved changes are promoted.

OBJECTIVE	REQUIREMENTS
	5. Emergency changes should be controlled through a separate emergency change process.
27. Ensure that Suppliers return or certify the destruction of all Confidential Information and Confidential Personal Information when it is no longer needed to provide goods or services to the firm.	1. All Confidential Information will be controlled and secured from the time it is created until it is destroyed, including off-site storage locations. 2. The physical disposal of any media that contains Confidential Information and Confidential Personal Information should be placed in locked receptacles and shredded. 3. Supplier will label any Sirva media with a generic name that does not allow a reader to infer that the media contains Confidential Information or Confidential Personal Information.
28. Ensure that locations that house computer systems, servers, voice or data network facilities, workstations, or Confidential Information and Confidential Personal Information are physically and environmentally secure. Prevent unauthorized access to information that is physically handled by personnel.	1. Supplier will maintain: a. Secure, physical separation between environments used to perform Sirva processing and environments used to perform processing for other customers. b. Appropriate physical security measures to ensure that only authorized personnel have access to the environment used to perform Sirva processing and computer hardware or other resources that house, access, or process Confidential Information. c. Access control devices on all entry points of Supplier's facility, with additional levels of segregation to sensitive areas. d. Generate, and review logs of all access control activities to the facility and to sensitive areas within the facility. e. Use of closed-circuit television surveillance equipment, personnel and/or monitoring devices to detect and provide the ability to investigate unauthorized or unusual access. Key areas to include for surveillance are: data centers/control centers, ingress/egress points to the data center/control center, generators or uninterrupted power supply (UPS) storage room. The recordings will be kept for a minimum of 90 days and will thereafter be securely deleted as and when reasonably designated by Sirva. 2. Visitors will be registered and sign in and out upon entry and should be escorted at all times. 3. Fire controls should provide automatic alerts that go directly to the fire department and have either automatic or manual suppression equipment. 4. Water-based fire systems should protect against accidental damage and/or leakage. 5. Supplier will provide power and air conditioning for critical processing components. 6. Supplier will provide for an alternate power source for power irregularities. 7. All service contract personnel, such as cleaning services and off-site storage services, should be bonded. 8. Paper and computer media containing Confidential Information will be stored in locked cabinets, rooms, and/or other forms of secured furniture or locations when not in use. 9. Policies, standards and/or procedures will be in place that instruct employees that Confidential Information will be removed from printers and fax machines immediately.
29. Ensure controls are in place to prevent malicious code.	1. Supplier will have established virus and security patch management processes that include the implementation of all industry-critical security patches within a prescribed timeframe for systems processing or storing Confidential Information and Confidential Personal Information. 2. Multiple products should be used to guard against malicious code such that no single vendor inherently is a single point of failure. 3. A malicious code program should be established, defining roles and responsibilities as well as events and responses to fully protect assets from damaging effects. 4. Emergency response procedures will be established and incorporated into overall security incident response procedures.

OBJECTIVE	REQUIREMENTS
30. Protect the Sirva environment by detecting potential security incidents and events and respond in a manner that minimizes impact and, if necessary, enables remedy via legal processes.	1. Event monitoring controls should be implemented on all configurable systems and devices housing applications, databases, servers, networking gear, and security. 2. All network traffic should be subject to event monitoring and analysis processes. 3. Applications and databases should provide logging for security events that can only be detected within the application or database. 4. Such security events will be documented. 5. Security event log thresholds may be defined, as needed, to facilitate effective log reviewing processes. 6. The following should be included in the log: a. Event Type. b. Time Stamp. c. Address information associated with the originating device (such as terminal ID, port number, network address and/or device name). d. System or information resource accessed in the event. e. Result of event. f. Reason for failure, relative to information protection requirements, as applicable to security event types resulting in failure. g. Old and new values associated with employee or customer relationship profile information, as applicable.
31. Establish and maintain a response capability to react to security incidents.	1. Security incident management will: a. Formally define roles and responsibilities. b. Assure minimum exposure to legal liability by preserving evidence associated to an incident. c. Define a communication plan to ensure full participation in incident resolution and full management awareness. 2. Alerts should be automatic that notify network managers of high risk or otherwise security related events. 3. The incident response policy and procedure should be documented and communicated. It should address: a. Roles and Responsibilities. b. Priority Levels. c. Incident Containment and Recovery. d. Communication. e. Management Reporting. f. Evidence Recovery and Preservation. g. Third Party (including law enforcement) coordination and communication. h. Root cause analysis.
32. Ensure that all email and messaging solutions are designed so that a failure of a single element does not put the core internal email or messaging servers at risk.	1. The use of electronic mail and instant messaging will be configured to ensure accountability for any Sirva business. 2. The use of Enforced TLS (Transport Layer Security) encryption. 3. Emails and instant messages will be retained for three years when conducting Security Exchange Commission (SEC) regulated business. Other regulatory retention requirements may apply. 4. The use of email filters to restrict unencrypted national identifiers (*e.g.*, social security numbers) and account numbers (*e.g.*, primary account numbers, credit card numbers, and debit card numbers) and other data elements of Confidential Information and Confidential Personal Information reasonably designated by Sirva from being sent.
33. Ensure recovery of Confidential Information in case of disaster or business interruption.	1. Supplier will adhere to agreed-upon contract requirements related to disaster recovery and business resumption plans. 2. Resiliency plans for services with a maximum allowable delay of 72 hours or less will be tested to assure business requirements can be met during an event that is disruptive to Sirva related services.

EXHIBIT B: MANDATORY GOVERNMENT CONTRACT FLOW DOWN PROVISIONS

APPLICABLE TO ALL SIRVA SUPPLIERS WORKING ON US FEDERAL GOVERNMENT AGENCY ASSIGNMENTS

PROVISION	TITLE/DESCRIPTION
FAR 52.203-6	Restrictions on Subcontractor Sales to the Government. States that contract cannot bar direct sales by subcontractor (or sub-subcontractor) to the government. Applicable to subcontracts that have value in excess of the simplified acquisition threshold (currently, $250,000).
FAR 52.203-7	Anti-Kickback Procedures. Imposes requirements that subcontractor have in place anti-kickback policies and imposes reporting requirements. Applicable to subcontracts that have value in excess of $150,000.
FAR 52.203-12	Limitation on Payments to Influence Certain Federal Transactions. Bars use of appropriated funds to lobby federal employees and members of Congress and imposes disclosure requirements. Applicable to subcontracts that have value in excess of $150,000 unless exempted.
FAR 52.203-13	Contractor Code of Business Ethics and Conduct. Requires adoption of code of conduct for subcontracts that have value in excess of $6 million and a performance of more than 120 days.
FAR 52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights. Makes subcontracts over the simplified acquisition threshold ($250,000) subject to the whistleblower protections in 41 USC 4712.
FAR 52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements. Prohibits restrictions on employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract.
FAR 52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities. Prohibits contractor/subcontractor from providing or using covered articles in the development of data or deliverables.
FAR 52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended or Proposed Debarment. Requires subcontractor to disclose whether it is debarred, suspended or proposed for debarment by the Federal Government. Applicable to subcontracts that have value in excess of $35,000 and are not for commercially available off-the-shelf items.
FAR 52.219-8	Utilization of Small Business Concerns. Implements government policies regarding small business concerns. Applicable to subcontracts that have value in excess of $700,000.
FAR 52.222-17, ¶ (l)	Non--displacement of Qualified Workers. Requires offers of employment to employees of prior subcontractors displaced by this contract. Applicable to subcontracts over simplified acquisition threshold (currently, $250,000).
FAR 52.222-21	Prohibition of segregated facilities. Prohibits segregated facilities based on race, color, religion, sexual orientation, gender identity or national origin.
FAR 52.222-26	Equal Opportunity. Implements government policies prohibiting discrimination based on race, color, religion, sex, sexual orientation, gender identity, or national origin.
FAR 52.222-35	Equal Opportunity for Veterans. Prohibits discrimination against qualified protected veterans and requires affirmative action in employment and advancement of qualified protected veterans. Applicable to subcontracts that have value in excess of $150,000 unless exempted.
FAR 52.222-36	Equal Opportunity for Workers with Disabilities. Prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action in employment and advancement qualified individuals with disabilities. Applicable to subcontracts that have value in excess of $15,000 unless exempted.
FAR 52.222-37	Employment Reports on Veterans. Requires annual reporting of veteran hires. Applicable to subcontracts that have value in excess of $150,000 unless exempted.

PROVISION	TITLE/DESCRIPTION
FAR 52.222-40	Notification of Employee Rights Under the National Labor Relations Act. Requires posting NLRA notice. Applicable to subcontracts that have value in excess of $10,000 and will be performed wholly or partially in the United States, unless exempted.
FAR 52.222-41	Service Contract Labor Standards. Sets requirements for compliance with minimum wage standards, safe and sanitary work environments, record-keeping requirements, etc. Applicability limited by FAR 52.222-53 if, among other things, work on government subcontract is less than 20% of worker's time.
FAR 52.222-50	Combating Trafficking in Persons. Prohibits trafficking in persons including for commercial sex acts and forced labor. Requirement for a compliance plan is limited to subcontracts in excess of $500,000.
FAR 52.222-54	Employment Eligibility Verification. Mandates compliance with e-verify rules for employees. Some exceptions may apply.
FAR 52.222-55	Minimum Wages Under Executive Order 14206. Requires specified minimum wage be paid to workers on federal contract.
FAR 52.222-62	Paid Sick Leave Under Executive Order 13706. Requires employer provide specified paid sick leave.
FAR 52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving. Encourages adoption of policy by contractor/subcontractor to ban text messaging while driving for government business. Applicable to subcontracts that have value in excess of the micro-purchase threshold (currently, $10,000).
FAR 52.223-99 (implementing Executive Order 14042)	Ensuring Adequate COVID Safety Protocols for Federal Contractors. Requires compliance with all guidance for workplace locations published by the Safer Federal Workforce Task Force available at https:/www.saferfederalworkforce.gov/contractors/.
FAR 52.224-2	Privacy Act. Requires compliance with the Privacy Act 5 USC 522a.
FAR 52.224-3	Privacy Training. Requires privacy training for employees with access to PII.
FAR 52.225-13	Restrictions on Certain Foreign Purchases. Prohibits purchase of supplies/services from countries subject to economic sanction.
FAR 52.244-6	Subcontracts for Commercial Items. Imposes requirement that subcontracts for commercial items, as defined in FAR 2.101, incorporate several additional contract clauses including, but not limited to, FAR 52.203-15 (Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009); FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems) and FAR 52.204-23 (Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities).
FAR 52.247-64	Preference for Privately Owned U.S.–Flag Commercial Vessels. Implements Cargo Preference Act that mandates shipping in 50% of cargo in US flagged ships; several exceptions apply.
EPAAR 1552.209-71	Organizational conflicts of interest. Requires disclosure of organizational conflicts of interest. Exceptions apply, including for simplified acquisition procedures.
EPAAR 1552.209-73	Notification of conflicts of interest regarding personnel. Requires disclosure of any actual or potential personal conflict of interest with regard to any employees working on contract. A personal conflict of interest is defined as a relationship of an employee, subcontractor employee, or consultant with an entity that may impair the objectivity of the employee, subcontractor employee, or consultant in performing the contract work.
HSAR 3052.209.72	Organizational Conflict of Interest. Prohibits conflicts of interest and imposes disclosure requirements. Applicable to subcontracts that have value in excess of the simplified acquisition threshold (currently, $250,000).
DJAR PGD 15-03	Security of Justice Department Information and Systems. Imposes requirements for protection of Department of Justice information. The full text of this clause is not contained in a published regulation but can be found here.

PROVISION	TITLE/DESCRIPTION
DTAR 1052.210-70	Contractor Publicity. Prohibits reference to supplies or services furnished pursuant to the contract in any news release or commercial advertising, or in connection with the same, without first obtaining explicit written consent from the Contracting Officer.
Access to Records	The Comptroller General or an appropriate Inspector General shall have access to and a right to examine subcontractor's records that pertain to the prime contract and to interview any officer or employee regarding such transactions.

DJAR-PGD-15-03 Security of Department Information and Systems

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. Information means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. Personally Identifiable Information (or PII) means any information about an individual maintained by an agency, including, but not limited to, information related 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 his or her 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.

C. DOJ Information means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. Information System means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. Covered Information System means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. [sic] Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the

request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat

vector, mitigation details, and all available incident details; and (4) any other information specifically requested by the DOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

EXHIBIT C: MANDATORY HONEYWELL FM&T CONTRACT FLOW DOWN PROVISIONS

APPLICABLE TO ALL SIRVA SUPPLIERS WORKING ON HONEYWELL FEDERAL MANUFACTURING & TECHNOLOGIES, LLC ASSIGNMENTS

Honeywell FM&T is a Management and Operating (M&O) Contractor for the U.S. Department of Energy (DOE). As such, it is required to flow down various provisions to its subcontractors, including Sirva, and Sirva is required to flow down these provisions to Sirva Suppliers who perform work on Honeywell FM&T assignments.

FAR AND DEAR CLAUSES/PROVISIONS & GOVERNMENT DIRECTIVES INCORPORATED BY REFERENCE

Applicable to all contracts, regardless of amount:

FAR 52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)
FAR 52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (JUL 2018)
FAR 52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (JUL 2018)
FAR 52.219-8	Utilization of Small Business Concerns (OCT 2018)
FAR 52.222-4	Contract Work Hours and Safety Standards Act--Overtime Compensation (MAY 2014)
FAR 52.222-21	Prohibition of Segregated Facilities (APR 2015)
FAR 52.222-26	Equal Opportunity (SEP 2016)
FAR 52.222-50	Combating Trafficking in Persons (with ALT I as applicable) (JAN 19)
FAR 52.244-6	Subcontracts for Commercial Items (AUG 2019)
FAR 52.225-1	Buy American – Supplies (MAY 2014)
FAR 52.225-13	Restrictions on Certain Foreign Purchases (JUN 2008)
FAR 52.227-3	Patent Indemnity (APR 1984)
FAR 52.227-14	Rights in Data-General (with ALT V and modified in accordance with 927.409(a)) (MAY 2014)
FAR 52.242-15	Stop Work Order (AUG 1989)
DEAR 952.203-70	Whistleblower Protection for Contractor Employees (DEC 2000)
DEAR 952.247-70	Foreign Travel (JUN 2010)
DEAR 970.5204-2	Laws, Regulations, and DOE Directives (DEC 2000) (Deviation)
DEAR 970.5245-1	Property (AUG 2016); "Government" remains unchanged.
DOE MEMO	DOE CIO Cybersecurity Action Memorandum dated October 5, 2018 regarding Prohibition on Acronis Branded Products/Services (OCT 2018)
DOE O 206.1	Department of Energy Privacy Program (JAN 2009)
DOE O 471.3	Identifying and Protecting Official Use Only Information (JAN 2011)

Applicable to all contracts regardless of amount:

…if funded under the Recovery Act

FAR 52.203-15	Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010)

…in all subcontracts except those for COTS items:

FAR 52.204-21	Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

…in all service contracts subject to the Service Contract Labor Standards Statute:

FAR 52.222-41	Service Contract Labor Standards (MAY 2014)

…in all service contracts subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute, and are to be performed in whole or in part in the US:

FAR 52.222-55	Minimum Wages Under Executive Order 13658 (DEC 2015)
FAR 52.222-62	Paid Sick Leave Under Executive Order 13706 (JAN 2017)

…if design, development or operation of a system of records on individuals is required to accomplish an agency function:

FAR 52.224-1	Privacy Act Notification (APR 1984)
FAR 52.224-2	Privacy Act (APR 1984)

…if subcontractor employees will: (1) Have access to a system of records, (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or (3) Design, develop, maintain, or operate a system of records:

FAR 52.224 -3 Privacy Training (JAN 2017)

…if FAR 52.224-3 is applicable and the agency specifies that only its agency-provided training is acceptable:

FAR 52.224 -3 ALT I Privacy Training (JAN 2017)

…if any contract work is subcontracted in accordance with FAR 48 CFR 52.227-3:

DEAR 970.5227-6 Patent Indemnity – Subcontracts (DEC 2000)

…if an uncleared contractor requires physical access to an NNSA site, logical access to NNSA Information Technology systems (including remote access), or a combination of both for greater than 179 days:

NNSA SD 206.2 Implementation of Personal Identity Verification for Uncleared Contractors (APR 2018)

…if supplies identified in the Schedule to be accorded duty-free entry will be imported into the customs territory of the United States; or, if other foreign supplies in excess of $15,000 may be imported into the customs territory of the United States:

FAR 52.225-8 Duty-Free Entry (OCT 2010)

…if the subcontractor is a small business:

FAR 52.232-40 Providing Accelerated Payments to Small Business Subcontractors (DEC 2013)

…if involving international air transportation:

FAR 52.247-63 Preference for U.S.-Flag Air Carriers (JUN 2003)

…if involving ocean transportation of supplies subject to the Cargo Preference act of 1954:

FAR 52.247-64 Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006)

…if performance involves risk of public liability for a nuclear incident or precautionary evacuation and Seller is not subject to Nuclear Regulatory Commission (NRC) financial protection requirements or NRC indemnification:

DEAR 952.250-70 Nuclear Hazards Indemnity Agreement (AUG 2016).

…when a major helium requirement is involved:

FAR 52.208-8 Required Sources for Helium and Helium Usage Data (APR 2014)

Applicable if the contract exceeds $3,500, is not a COTS item and includes work to be performed in the United States:

FAR 52.222-54 Employment Eligibility Verification (OCT 2015)

Applicable if the contract exceeds the Micro-Purchase Threshold:

FAR 52.223-18 Encouraging Contractor policies To Ban Text Messaging While Driving (AUG 2011)

Applicable if the contract exceeds $10,000 and will be performed wholly or partially in the United States:

FAR 52.222-40 Notification of Employee Rights Under the National Labor Relations Act (DEC 2010);

Applicable if the contract exceeds $15,000:

FAR 52.222-20 Contracts for Materials, Supplies, Articles, and Equipment Exceeding $15,000 (MAY 2014).

FAR 52.222-36 Affirmative Action For Workers With Disabilities (JUL 2014)

Applicable if the contract exceeds $150,000:

FAR 52.203-7 Anti-Kickback Procedures (MAY 2014)

FAR 52.203-12 Limitation on Payments to Influence Certain Federal Transactions (OCT 2010)

FAR 52.222-35 Equal Opportunity for Veterans (OCT 2015)

FAR 52.222-37 Employments Reports on Veterans (FEB 2016)

…and subcontractor employees will perform acquisition functions closely associated with inherently governmental functions:

FAR 52.203-16 Preventing Personal Conflicts of Interest (DEC 2011)

Applicable if the contract exceeds the Simplified Acquisition Threshold as defined in FAR 2.101:

FAR 52.203-6 Restrictions on Subcontractor Sales to the Government (SEP 2006)

FAR 52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights (APR 2014)
FAR 52.227-1	Authorization and Consent (DEC 2007)

…and is for services:

FAR 52.222-17	Non-displacement of Qualified Workers (MAY 2014)

…and involves the performance of advisory and assistance services:

DEAR 952.209-72	Organizational Conflicts Of Interest (AUG 2009), ALTERNATE I. (b)(1)(i) Period is 'five (5) years'

…and support operations of the DOE facility and offers significant subcontracting opportunities for energy efficient or environmentally sustainable products or services:

DEAR 952.223-78	Sustainable Acquisition Program (OCT 2010)

Applicable if the contract exceeds $700,000, and the subcontractor is not a small business:

FAR 52.219-9	Small Business Subcontracting Plan (AUG 2018)

Applicable if the contract exceeds $500,000, and is for services:

FAR 52.204-14	Service Contract Reporting Requirements (OCT 2016)

Applicable if the contract exceeds $5,500,000, and has a performance period of more than 120 days:

FAR 52.203-13	Contractor Code of Business Ethics and Conduct (OCT 2015)