1. **TECHNOLOG****Y USAGE**
* IT Travel Protocol
* Antivirus
* Social Media and Web Usage
* Access Request Form
* New Employee Default Access
* Internet Usage

**USSEC IT Travel Protocol**

**Summary**

In-house computers and servers have the benefit of physical security protection as well as on-site staff to help ensure they remain safe and uncompromised. Traveling with USSEC property and/or data can pose a special risk to employees as well as the organization if the devices and/or information contained thereon become lost or stolen. It is critical for staff to follow specific guidelines to minimize this risk so they can perform their job functions and still adhere to good security practices which protect USSEC.

**Purpose**

USSEC’s IT Travel Policy exists to protect data security and USSEC’s systems, networks, and information from unauthorized access while off business property.

**Scope**

Every officer, director, manager, employee, contractor, temporary worker, authorized agent, and volunteer who has a smartphone, tablet computer or laptop, whether purchased personally, by USSEC, or by a third party, is subject to the terms of USSEC’s IT Travel Policy.
Note that for the purpose of this policy the term “portable device” refers to USSEC-owned smartphones, tablet computers and laptops OR employee-owned devices which contain USSEC information, such as email or data files.

**Exceptions**

There are no exceptions to this policy.

**Approved IT Travel Standards**

These standards are broken down into three categories:

1. Steps to take before travel
2. Steps to take during travel
3. Steps to take after travel

Furthermore, there is a different set of risks involved with international travel compared to domestic, so guidelines for each are listed where relevant.

Before traveling (applies to both domestic and international travelers)

* No single copy of data is to be stored on any portable device—primary copies must be kept on an internal server.
* No personal identifier data such as social security numbers, driver’s license numbers or bank/credit card numbers are to be kept on portable devices.
* Only take the minimum amount of data when traveling. Consider whether you can connect to company resources via a remote virtual private network (VPN) connection or terminal server and access data at the office, which would eliminate the need to store any information on the portable device.
* Do not plan to bring printouts of any company data except marketing/presentation material which does not constitute sensitive information.
* No devices should be shared with other employees or non-company personnel.
* It is recommended that employees change their passwords immediately before travel.
* All portable devices must be secured via a password/PIN.
* All laptops must have antivirus/firewall protection and current application/operating system patches installed.
* Pack laptops in foam, bubble wrap, or appropriate computer case/bag to protect them during transit.
* Shut down laptops before traveling—do not put them to sleep or in hibernation, since this may facilitate unwarranted access.
* Arrange for a locked case to carry portable devices if not in your possession at all times.
* If possible, arrange for a portable mi-fi or tethering via a device equipped with internet access so you can avoid using unknown networks during travel.

### Pre-travel Requirements for International Travelers

* Bring proof of ownership of portable devices to present to US Bureau of Customs & Border Protection (CBP) personnel upon re-entering your native country.
* If proof of ownership does not exist, these devices should be registered with the CBP before departing via registration form [CBP form 4457](http://forms.cbp.gov/pdf/CBP_Form_4457.pdf).
* It is also recommended that you obtain a letter signed by a USSEC official stating you are permitted to take USSEC property while traveling internationally and the computer/software complies with the
[Export Administration Regulations of the United States](http://forms.cbp.gov/pdf/CBP_Form_4457.pdf).
* Keep in mind CBP officers have the right to examine the contents of your portable devices and confiscate them if desired.
* Exercise caution when planning travel to potentially unstable countries such as Syria or North Korea.
* It is presently recommend against bringing a laptop to China due to the hacking risk.
* Make sure to bring power adapters which are compatible with the country to which you are traveling.

### During Travel

* Portable devices are to be kept under your control at all times (do not check, ship or give to anyone else for transport).
* Laptops must be stored in cases while in transit.
* Keep in mind that airports, train stations, bus terminals and other high-traffic travel areas can be particularly dangerous places in terms of loss or theft. Exercise special caution in these areas.
* It is acceptable for security personnel to x-ray portable devices. However, metal detectors can harm these objects so travelers should request visual inspections instead.
* Do not leave portable devices visible in unattended vehicles, even if locked.
* Do not leave portable devices unprotected in hotel rooms—use a safe or a security cable.
* Do not connect to unsecured networks—only connections to appropriate secured networks (such as hotel wi-fi or company mi-fi devices) are suggested.
* Access to company resources over public computers (such as public internet terminals) is prohibited.
* If possible, copy any updated information back to internal servers periodically via secure means such as VPN connections.
* Notify your manager as well as the IT department immediately if a device is lost or stolen.

### After Traveling

* Employee passwords should be changed.
* All company data should be copied back to an internal server or removed entirely in the case of external USB drives.
* Systems should be securely erased then reimaged if there is a concern about compromised access.

### Monitoring

Use of USSEC computer devices can be monitored at any and all times and the associated content inspected by approved personnel upon request to ensure compliance.

### Violations and Penalties

Any violation of the USSEC IT Travel Policy must be immediately reported to the appropriate department manager and IT Manager. Violating the USSEC IT Travel Policy or any of its tenets could result in disciplinary action leading up to and including termination of employment and **civil and/or criminal prosecution under local, state, and federal laws.**

### Acknowledgment of IT Travel Policy

This form is used to acknowledge receipt of and compliance with USSEC’s IT Travel Policy.

Procedure

Complete the following steps:
1. Read the IT Travel Policy.
2. Sign and date this form in the spaces provided below.
3. Return this page only to the HR department manager.

Signature

By signing below, I agree to the following terms:

(i) I have received and read a copy of the IT Travel Policy and understand and agree to the same.

(ii) I understand USSEC may monitor the implementation of and adherence to this policy to review the results for accuracy.

(iii) I understand and agree to document exceptions to this policy and obtain managerial approval as required.

(iv) I understand that grave violations of the IT Travel Policy could result in termination of my employment and legal action against me.

Employee Signature

Employee Name

Employee Title

Date

Department/Location

**USSEC IT Anti-Virus Protocol**

**Summary**

Computer viruses (also known as “malware”) are malicious self-replicating programs which can infect files. A virus can steal information, send out junk email and damage programs/operating systems. Viruses disrupt computers, cause needless downtime, consume staff resources and pose significant security risks to the organization.
Viruses can enter a network via the follow methods:

* Email—viruses can be sent as email attachments pretending to be documents, spreadsheets, pictures, jokes, etc. Infected attachments may be sent with or without the knowledge of the sender. Once opened, viruses infect unprotected systems then can replicate through email or across the network without the recipient’s knowledge.
* Software downloaded from the Internet—Downloaded software can contain viruses, particularly from disreputable sites such as those offering shared files or pirated software.
* Disks, CDs, flash drives, or other media—Storage media can also be a source of viruses, especially from unknown sources.
* Instant messaging attachments—Viruses can be transmitted through instant messaging software either directly or via clickable internet links.
* Outside computers brought into the company—A vendor laptop plugged into the network to conduct a presentation can introduce a virus to the organization. Furthermore, a company laptop brought home then back to the office the next day can pose a threat if it has been infected in the interim.

Anti-virus applications protect the business by keeping systems and networks free of malware, and are especially critical for PCI-compliant status (if applicable). This policy will define how anti-virus protection is to be deployed throughout the USSEC organization.

### **Objective**

This policy outlines the methodologies to be used in applying, supporting and maintaining anti-virus applications on USSEC workstations and servers.

### **Audience**

This policy applies to all company employees, whether using work computers or personal systems to access company resources. Windows, Mac and Linux operating systems are included in these requirements.

### **Exceptions**

All USSEC workstations and servers are required to use updated anti-virus applications. Exceptions to this rule are permitted only in cases where anti-virus software is not feasible (for performance/application compatibility reasons or lack of applicable options, such as on certain older server operating systems) and must be documented/approved by the IT Manager. In these rare instances, the excluded systems would reside on separate subnets with only specific traffic permitted to the rest of the organization.

###

### **Anti-virus Policy Requirements**

Administrators should adhere to a combination of standards to ensure the maximum defense possible against viruses. These include policies for categories such as security, anti-virus settings, scanning, email, signature updates, user education and anti-virus detection/ removal steps.

**Security Policies**

* Regular installation of operating system and application patches are performed. In many cases, viruses prey upon vulnerabilities which can be corrected before infection.
* Scheduled regular data file backups and tests of results to ensure information can be restored if needed.
* Only necessary firewall ports are open between the internet and internal USSEC network.
* All non-company workstations must be connected to a separate wireless network DMZ or a direct connection to the internet; these must never be placed on the same subnet as company systems.
* Remote users (such as those who connect by virtual private network or VPN) connect to a segregated network subnet even if using company hardware. A firewall protects the main company subnet with only permitted ports opened to the main network to reduce the impact of a compromised computer on the VPN.
* Limited internet access to approved sites through use of USSEC web filter.
* Applications restricted to the specific job duties of employees. USSEC does not allow any software to be installed beyond that provided with their system or which is approved for use thereafter by the IT Manager.

**Anti-virus Setting Policies**

* Administrators should understand that not all viruses will be detected/blocked by a single product. USSEC uses multilayered defenses such as anti-virus scanning on email and file servers in addition to workstation anti-virus protection.
* The appropriate anti-virus packages are implemented on USSEC servers based upon the products they use. For instance, email servers have designated email anti-virus software.
* Software is used that allows files to be quarantined if they cannot be repaired to prevent users from gaining access to the infected files and perpetuating the virus.
* Anti-virus software is configured so it cannot be disabled, stopped or removed without an admin password.
* Macro virus-protection is active within software packages such as Word and Excel.

**Scanning policies**

* All systems configured to run full anti-virus scans on a weekly basis.
* Scheduled scans to occur during times of minimal use (such as off-hours) for minimal performance impact.
* Scans performed in “stealth mode” to help further improve system performance.
* User intervention of scans is disabled.
* Background monitoring (“autoprotect”) on the workstations so files are scanned on-access enabled.
* All file types included when scanning, such as .exe, .dll, and .zip files.
* Web filter to scan online files prior to downloading.

**Email policies**

* USSEC subscribes to a third party email scan service to utilize dedicated email gateways to process messages for malware and keep it from entering the network in the first place.
* Email server filters to eliminate spam and unsolicited junk email that could contain malware.
* Scanning of all incoming and outgoing email and attachments.
* Executable file attachments are blocked from being transmitted, such as .exe, .vbs, .bat and .com files.
* Email server configured with anti-virus to quarantine suspicious messages/attachments and notify administrators/ recipients that these have been blocked.
* Non-work-related downloading of attachments is prohibited.
* Forwarding jokes or chain letter emails is prohibited.

**Anti-Virus Signature Updates**

* All servers and workstations receive daily signature updates.
* A dedicated server is setup to retrieve regular updates and distribute these to USSEC internal systems.
* Remote systems which may only contact the company sporadically (such as those used by traveling employees) are also set up to retrieve signature updates directly over the internet.
* Alerts are enabled to notify users and administrators when anti-virus signatures are outdated.
* Reports on USSEC anti-virus updates are reviewed to ensure these are working as expected.

**User Education**

* Mandated for users to install a trusted anti-virus software package on any home computers which will be used for USSEC purposes, such as those connecting to the VPN or TERMSRV3.
* Mandated for users to report when they find a virus on their system so it can be tracked which viruses surfaced in USSEC’s network.
* Users will be informed of new virus threats and spam threats to heighten their sense of awareness.

**Anti-virus Detection/Removal**

* If a virus is found in an incoming email, the spam filter will blackhole the email.
* Anti-virus software configured to quarantine or repair infected files. Users are not permitted to choose which actions to take.
* If a virus is detected but cannot be quarantined or removed, the computer will be immediately taken offline and repaired.
* If the virus has impacted a Windows system, it will be rebooted into safe mode to minimize interference from the virus when attempting removal.
* If the anti-virus program is not functioning, it may be compromised or damaged. In this situation the computer will be booted with a portable operating system (which includes an anti-virus scanner) that can be updated online then used to scan the hard drive. If this is not possible, the affected system’s hard drive will be removed and cleansed from another computer.
* If the hard drive cannot be removed or scanned elsewhere an online virus scanner such as Trend Micro’s [HouseCall](http://housecall.trendmicro.com/) can be used on the impacted system. In this scenario the system must be hooked up to the public network and not the internal USSEC network. Keep in mind that viruses can damage or redirect web browsers so a portable web browser such as Firefox or Chrome may be needed for this endeavor.
* Reimage or reinstallation the operating system will occur if the virus cleansing operation is considered less than 100 percent successful. It is always better to format and start over rather than risk an ongoing contamination.
* If multiple workstations are impacted by a virus, there may be an outbreak. If more than two reports of a virus occur within a few minutes it may be necessary to shut down USSEC workstations or servers to contain the damage while the targeted systems are disinfected. This will be the judgment call of
the IT Manager.

**Reporting virus threats**

Users should become familiar with their anti-virus applications and report any issues to the IT department. Errors or the malfunction/disappearance of anti-virus software can indicate a malware threat is present. Similarly, be skeptical of any unknown program or internet site which claims it has found a virus on your system and offers to clean it for you—particularly if a fee is involved. When in doubt contact the IT department.

* If a virus is found which impacts a critical document, USSEC anti-virus software will attempt to clean the file. If this is not possible the file will be removed. In this case the last possible backup will be used to recover the infected file.
* IT staff will assume responsibility for notifying the user community of malware threats.
* Employees should not send out virus warnings, no matter how well-intentioned, as these can involve urban legends, old threats long since rectified, and can even further spread an infection.

### **Monitoring**

Use of anti-virus software can be monitored at any and all times, and all USSEC company data and systems can be scanned by approved personnel/software as needed.

**Practice Safe Computing**

USSEC users must take all necessary steps to prevent virus outbreaks. Use the following rules when operating your computer:

* Never open an email or instant-messaging attachment from an unknown or suspicious source.
* Do not open suspicious email attachments, even from coworkers.
* Be wary of clicking on links in emails/instant messages. It is better to hover your mouse pointer over a link. This will show you the true address behind the link.
* Only visit known and trusted websites.
* Do not use outside computers on the USSEC network.
* Do not allow outside users access to the USSEC network
* Do not allow un-approved technicians access to USSEC hardware or the USSEC network.
* Do not use USSEC computers (such as laptops) on untrusted networks or use them for non-USSEC purposes.
* Do not attach foreign networking devices, such as hotspots, to the USSEC network
* Do not attempt to bypass USSEC’s web filter or use proxy servers

### **Violations and Penalties**

Any violation of the Anti-virus Policy must be immediately reported to the IT Manager and the employee’s manager. Violating the Anti-Virus Policy or any of its tenets could result in disciplinary action leading up to and including termination of employment.

### **Acknowledgment of Anti-virus Policy**

This form is used to acknowledge receipt of and compliance with USSEC’s Anti-Virus policy.

**Procedure**

Complete the following steps:
1. Read the Anti-Virus Policy.
2. Sign and date this form in the spaces provided below.
3. Return this page only to the HR department manager.

**Signature**

By signing below, I agree to the following terms:

(i) I have received and read a copy of the Anti-Virus Policy and understand and agree to the same.

(ii) I understand and agree that any software and hardware devices provided to me by the company
are to be used for company business and not recreational purposes.

(iii) I understand and agree that I am not to modify, alter, or upgrade any software programs or hardware devices provided to me by the organization without the permission of the information technology department.

(iv) I understand and agree I must make reasonable efforts to protect all company-provided software and hardware devices from virus infection.

(v) I understand that if I break policy and bring a virus into the organization, I may be subject to disciplinary action up to and including termination. Furthermore, I will assume responsibility for any lost data eradicated by anti-virus programs which cannot be recovered.

Employee Signature

Employee Name

Employee Title

Date

Department/Location

**USSEC Social Media and Web Usage Protocol**

**Summary**

Social Media and Web interactions are now standard procedures for customer-engaged companies and their employees. Blogs, website comments, Facebook, Twitter, LinkedIn, Instagram and Google+ are several examples of sites and services which businesses rely on in order to share public information, build customer relationships and obtain relevant feedback. The nature of open participation within these mediums allows for ongoing dialogue with customers in a mutually beneficial exchange of ideas. These resources are frequently used by company employees both inside and outside of the scope of their duties and at times the lines of interaction with internal and external individuals can become blurred.
Given the high-profile nature of social media and the web, it is essential that company staff engage in responsible online activities which represent themselves and USSEC with utmost honesty and professionalism.

**Purpose**

The purpose of this policy is to provide guidelines for appropriate behavior for USSEC employees when interacting with others via social media and the web, whether on behalf of USSEC or during their own personal endeavors. These rules are to protect both USSEC and its employees.

**Scope**

All full-time employees, contract workers, consultants, part-time staff, temporary workers and other personnel.

### **Exceptions**

There are no exceptions to this policy.

### **Approved Social Media and Web Usage**

Only official or approved accounts may be used when interacting on social media or the web to conduct USSEC business or discuss USSEC or it’s employees in any way. These account passwords must be different from those of internal accounts and documented.

Only authorized employees have permission to:

* Represent USSEC online.
* Announce or report on USSEC activities.
* Comment on USSEC’s products, performance, personnel or decisions.
* Respond to requests for information from outside individuals such as journalists, competitors, or other agencies (unauthorized employees must report and refer these incidents to their manager for the appropriate escalation where applicable).
* Comment or discuss any USSEC board member, employee, contractor or temporary worker.

Authorized employees should follow these procedures:

* Identify themselves as an employee when discussing or commenting on any online topic related to USSEC.
* Employ a disclaimer stating that their opinions are theirs alone and are not intended to represent those of USSEC.
* Post only public information or information which is authorized for release and known to be factual. In the event something believed accurate is found to be invalid this material must be retracted and/or corrected.
* Never reveal or discuss confidential and/or proprietary information such as trade secrets, intellectual property, personally identifiable information or any material protected by copyright, patent, or that which is otherwise legally protected.
* Do not utilize profanity or make inflammatory, racial, sexual or otherwise discriminatory/inappropriate comments.
* Do not become involved in political, religious or other controversial and potentially provocative topics unless for explicitly approved business purposes.

All employees whether authorized or unauthorized should adhere to these concepts when using social media and the web:

* Do not utilize USSEC logos/trademarks online without approval.
* Do not post anonymously when discussing USSEC products, personnel, services or other details.
* Do not discuss or refer to clients/customers, partners or other USSEC-related individuals and entities without approval.
* Do not discuss USSEC activities or personnel in any way
* Do not tag, mention or otherwise refer to USSEC employees on social media without their consent. This includes pictures, check-ins and LinkedIn recommendations.
* Consider and avoid “conflict of interest” situations such as sending friend or connection requests to customers, supervisors or subordinates.
* Adhere to any existing restrictions such as those enforced by non-compete and non-solicit agreements; for instance, if prohibited from recruiting competitor employees do not use LinkedIn to attempt to do so.
* Obey laws such as those prohibiting insider training, harassment, defamation and discrimination.
* When interacting with other employees on social media sites, adhere to the same guidelines as those applied within the physical office space. Harassing, bullying and unprofessional behavior, or that which otherwise makes others uncomfortable will not be tolerated and may be subject to HR review and action.
* Report to your manager any false, defamatory or other negative material posted online about USSEC (whether presented by company or non-company personnel). Do not respond to this content unless authorized to do so.

It is understood that employees will have separate professional and personal lives and USSEC cannot restrict what they do on social media on their own time with their own accounts/equipment. However, use of these personal accounts during USSEC business hours or with USSEC issued equipment, or discussing or posting about USSEC activities or USSEC staff is strictly prohibited.

Because the online reputation of individuals can often be linked with their employers, we request employees to show good judgment when using social media and web services no matter the nature of their activities. For example, please do not post offensive images or content or reveal personal information which might put you a risk for identity theft or other criminal activities.

### **Monitoring**

The use of USSEC computers or smart devices for personal social media activities falls under the same guidelines applied by the USSEC Internet Usage Policy. Employees should understand that this access should not interfere with their work responsibilities, it is monitored and will be reviewed at any time upon managerial discretion.

### **Violations and penalties**

Any violation of the Social Media and Web Policy must be immediately reported to the employee’s manager and any related departments (such as Marketing for instance). Violating the Social Media and Web Policy or any of its tenets could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under local, state, and federal laws.

### **Acknowledgment of Social Media and Web Usage Policy**

This form is used to acknowledge receipt of, and compliance with, USSEC’s Social Media and Web Usage Policy.

**Procedure**

Complete the following steps:
1. Read the Social Media and Web Usage Policy.
2. Sign and date this form in the spaces provided below.
3. Return this page only to the HR department manager.

**Signature**

Your signature attests that you agree to the following terms:

(i) I have received and read a copy of the Social Media and Web Usage Policy and I understand and agree to the same.

(ii) I understand USSEC may monitor the implementation of and adherence to this policy to review the results for appropriateness of content.

(iii) I understand that violations of the Social Media and Web Usage Policy could result in termination of my employment and legal action against me.


Employee Signature

Employee Name

Employee Title

Date

Department/Location

### **ADDITIONAL ACCESS RIGHTS APPROVAL PROCESS**

As a user’s role changes and naturally evolves, access to new or additional USSEC resources may be required. An end user requiring additional access permissions should forward the following information to his/her department manager:

• User’s full name

• Directory, system, application or data share access and/or permissions being requested

• Business justification for request

• User’s email address

• User’s department

The end user’s manager must first approve the additional access rights. Certain requests may require approval by the CPO, or department equivalent. The end user’s manager will obtain higher approval if needed.

Upon approving the expanded permissions, the manager will then forward the access rights request, via email, to the information technology manager for implementation.

**USSEC NEW EMPLOYEE CHECKLIST AND DEFAULT ACCESS POLICY**

**Summary**

The New Employee Checklist and Default Access Policy simplifies the process of accommodating new hires. By listing the elements that must be reviewed with each new staff member, and by assigning default access permissions enabling end users to best perform business-related tasks, USSEC helps ensure new employees experience standardized and consistent orientation and receive appropriate access rights.

**Purpose**

The New Employee Checklist and Default Access Policy enables the Information Technology and Human Resources departments to effectively and efficiently partner and ensure new hires receive orientation materials and information technology policy guidance. The New Employee Checklist and Default Access Policy also describes and establishes the primary level of systems access each end user receives, while reviewing the process end users should follow to request and receive additional access as a user’s roles and responsibilities naturally change and evolve.

**Scope**

The New Employee Checklist and Default Access Policy covers every USSEC director, manager, employee, contractor, temporary worker, authorized agent, intern and volunteer.

**New Employee Checklist**

The following checklist provides a simple chart that Information Technology and Human Resource representatives should leverage whenever introducing a new employee to USSEC’s information technology policies and procedures.

INFORMATION TECHNOLOGY

* Assign telephone and extension
* Create Active Directory user account
* Create electronic mailbox
* Assign group memberships:
	+ Accounting
	+ Communications
	+ Contracts
	+ Executive
	+ Human Resources
	+ Information Technology
	+ Marketing
* Assign workstation/laptop
* Assign Smartphone (if applicable)
* Assign tablet computer (if applicable)
* Enable remote access (if applicable)
* Provision all equipment:
	+ Applications (Smartphone, tablet, desktop and laptop)
	+ Email
	+ Proprietary software programs
	+ Printers
	+ Remote Connectivity
* Assign door/access security code
* Distribute, review and execute IT policies and procedures
* Issue magnetic badge
* Review information security requirements

Once contacted by the hiring manager, the information technology department will supply hardware for new end users within one week of receiving such requests.

### **Default Access Details**

When an individual becomes an employee or an approved volunteer or begins working with USSEC as a contracted employee, the information technology department assigns predefined network and systems access for the user. This policy outlines the basic access provisioned for each user.
All end users receive the following access to network resources upon request by the department manager:

* Account/Network Logon – A username and default password will be created for the user. At the first login, the end user will select a password that meets the minimum password requirements.
* Email – An email address will be provided to the end user using the default naming convention of USSEC.
* Departmental Directories – An end user will inherit read/write access to any folders owned by his or her department.
* Home Folder (H DRIVE)– The My Documents folder associated with the end user’s logon information will be created on the network, allowing documents created by a staff member to be stored on a network server and backed up.
* Intranet – All end users receive permission to access the organization’s internal network designed for organization communication, team collaboration and file access.
* Organization Forms – An end user will inherit read access to all global company folders containing such information as time sheets, vacation slips, expense forms, employee handbooks, benefits information, information technology policies and procedures, etc.
* Printers – Access to printers nearest an end user’s workstation will be automatically provided.
* Telephone – All new employees will receive a voice mailbox and telephone extension.
* Time and Attendance – New users will be given access to all time and attendance systems and payroll applications.
* Webmail – Each user possessing an email account also receives permission to access the organization’s Web-based email portal. https://mail.ussec.org/owa

### **Additional Access Rights Approval Process**

As a user’s role changes and naturally evolves, access to new or additional USSEC resources may be required. An end user requiring additional access permissions should forward the following information to his/her department manager:

• User’s full name

• Directory, system, application or data share access and/or permissions being requested

• Organization resources, systems or networks to which the user wishes to connect

• Business justification for request

• User’s email address

• User’s department

The end user’s manager must first approve the additional access rights. Upon approving the expanded permissions, the manager will then forward the access rights request, via email, to the information technology director for implementation.

### **Orientation Signatures**

The Information Technology and Human Resources representatives that complete the above section reviews with the new employee must sign this New Employee Checklist and Default Access Policy below and file this completed form in the new employee’s permanent human resources department file.

|  |
| --- |
|  |
| New Employee Name: |  |
| Hire Date: |  |
| New Employee Department |  |
|  |  |
|  |  |
| Human Resources Representative: |  |
| HR Review Tasks Completion Date: |  |
| HR Representative Signature: |  |
| Information Technology Representative: |  |
| IT Review Task Completion Date: |  |
| IT Representative Signature: |  |

#### **Acknowledgment of New Employee Checklist and Default Access Policy**

This form is used to acknowledge receipt of and compliance with USSEC’s New Employee Checklist and
Default Access Policy.

Procedure

Complete the following steps:
1. Read the New Employee Checklist and Default Access Policy.
2. Sign and date this form in the spaces provided below.
3. Return this page only to the HR department manager.

Signature

By signing below, I agree to the following terms:

(i) I have received and read a copy of the New Employee Checklist and Default Access Policy;

(ii) I understand and agree that I am not to attempt to connect to USSEC systems, networks and/or data without the express written permission of my departmental manager;

(iii) I understand and agree that I am to follow the above-described access rights process to receive new permissions and have the new permissions approved by my department manager whenever I wish to receive additional or new access permissions;

(iv) I understand and agree only the USSEC’s information technology manager is to implement additional access permissions and these access permissions must first be approved by my department manager;

(v) I understand and agree that any violation of the New Employee Checklist and Default Access Policy could result in termination of my employment and civil and criminal penalties.

Employee Signature

Employee Name
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Employee Title

Date
Department/Location

**USSEC Internet Usage**

**Summary**

The Internet is a constantly growing worldwide network of computers and servers that contain millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. Users are further cautioned that it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content.

**Purpose**

Employees and users accessing the Internet do so at their own risk and understand and agree that USSEC is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at USSEC is governed by this policy.

**Scope**

All full-time employees, contract workers, consultants, part-time staff, temporary workers and other personnel.

**Exceptions**

There are no exceptions to this policy.

**Approved Internet Usage**

The computer network is the property of USSEC and is to be used for legitimate business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain Users may also be provided with access to the Internet through the DMZ guest wireless network. All Users have a responsibility to use USSEC’s computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, up to and including termination, and civil and/or criminal liability.

**PROHIBITED ACTIVITIES**

Without prior written permission from USSEC, the network and/or USSEC computer hardware may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials.

Occasional limited, appropriate personal use of USSEC computer or smart device hardware is permitted if such use does not:

• Interfere with the User's or any other employee's job performance.

• Have an undue effect on the computer hardware or USSEC’s network performance.

• Violate any other policies, provisions, guidelines or standards of this agreement or any other of USSEC.

At all times users are responsible for the professional, ethical and lawful use of the USSEC network and USSEC computer systems. Personal use of computer hardware is a privilege that may be revoked at any time.

**ILLEGAL COPYING**

Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the IT Department.

**COMMUNICATION OF TRADE SECRETS**

Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to USSEC. Unauthorized dissemination of such material may result in severe disciplinary action, termination of employment, as well as substantial civil and criminal penalties under State and Federal Economic Espionage laws.

**ACCESSING THE INTERNET**

To ensure security, avoid the spread of viruses & malware, and maintain USSEC’s Internet Usage Policy, employees may only access the Internet through a computer attached to USSEC’s network and approved Internet firewall and web filter.

Bypassing USSEC’s network security by accessing the Internet directly with personal connections such as (but not limited to) Cellular Networks, mobile hot-spots, modems, foreign networking devices or proxy avoidance techniques or by any other means is strictly prohibited.

**FRIVOLOUS USE**

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others.

These acts include, but are not limited to:

• Sending mass mailings or chain letters

• Spending excessive amounts of time on the Internet

• Playing games

• Engaging in online chat groups or other social media

• Engaging with or posting to social media platforms or sites

• Uploading or downloading large files

• Accessing streaming video files

• Creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

**VIRUS DETECTION**

Files can be obtained from sources outside USSEC, including:

• Drives or disks brought from home

• Files downloaded from the Internet, newsgroups, bulletin boards, or other online services

• Files attached to e-mail

• Files provided by customers or vendor

These files may contain dangerous computer viruses that may damage USSEC’s computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use drives/disks from non-USSEC sources. If you suspect that a virus has been introduced into USSEC’s network or hardware, notify the IT Department immediately

**Monitoring**

NO EXPECTATION OF PRIVACY

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using the USSEC’s computer equipment. The computer network is the property of USSEC and may be used only for USSEC purposes.

Users expressly waive any right of privacy in anything they create, store, post, send or receive using USSEC computer equipment, portable devices or Internet access.

Note that for the purpose of this policy the term “hardware” refers to USSEC-owned smartphones, tablet computers and laptops OR employee-owned devices which contain USSEC information, such as email or data files.

Users consent to allow USSEC personnel access to and review of all materials created, stored, sent or received by User through any USSEC hardware, network or Internet connection.

USSEC has the right to monitor, log and archive any and all aspects of its network and computer hardware including, but not limited to:

• Monitoring Internet sites visited by Users

• Monitoring chat and newsgroups

• Monitoring file downloads

• Monitoring print jobs

• Monitoring communications sent and received by users via:

o Email

o File Transfer

o IM & Chat

o Phone Calls

o Social Networking

Employees should understand that this access should not interfere with their work responsibilities, it is monitored and will be reviewed at any time upon managerial discretion.

USSEC has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

Access to these types of sites is strictly prohibited:

• Drug Abuse

• Hacking

• Illegal or Unethical

• Discrimination

• Violence

• Proxy Avoidance

• Plagiarism

• Child Abuse

• Alternative Beliefs

• Adult Materials

• Advocacy Organizations

• Gambling

• Extremist Groups

• Nudity and Risqué

• Pornography

• Tasteless

• Weapons

• Sexual Content

• Sex Education

• Alcohol

• Tobacco

• Lingerie and Swimsuit

• Sports

• Hunting

• War Games

• Online Gaming

• Freeware and Software Downloads

• Streaming Media

• Peer-to-peer File Sharing

• Internet Radio or TV

• Internet Telephony

• Online Shopping

• Malicious Websites

• Phishing

• SPAM

• Advertising

• Brokerage and Trading

• Web-Based Personal Email

• Entertainment

• Arts and Culture

• Education

• Health and Wellness

• Job Search

• Medicine

• News and Media

• Social Networking

• Political Organizations

• Reference

• Religion

• Personal Vehicles

• Dynamic Content

• Folklore

• Web Chat

• Instant Messaging or IM

• Newsgroups and Message Boards

• Digital Postcards

• Real Estate

• Personal Websites or Blogs

• Content Servers

• Domain Parking

• Personal Privacy

• Search Engines and Portals

• Web Hosting

• Secure Sites

• Web-based Applications

**Violations and Penalties**

Any violation of the Internet Usage Policy must be immediately reported to the employee’s manager and any related departments. Violating the Internet Usage Policy or any of its tenets could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under local, state, and federal laws.