2016-2017 Antarctica Deployment Packet for ASC Personnel

Please review this Deployment Packet carefully. It includes information you need to know before you get to the Ice and the forms you'll need to fill out and mail or fax to ASC.

Photo Credit: Deven Stross

Antarctic Support Contract
7400 S. Tucson Way
Centennial, CO 80112-3938

Travel:
800-688-8606 x33202
303-790-8606 x33202
fax: 303-705-0742
email: deploy@usap.gov

Medical - UTMB:
855-300-9704
fax: 409-772-3600
email: medical@usap.gov

HR - Best Recycling:
800-688-8606 x32214
720-568-2214

HR - Gana-A'Yoo (GSC):
800-688-8606 x32494 or 32120
720-568-2494
720-568-2120
fax: 303-662-8770

HR - GHG:
800-688-8606 x32138
720-568-2138
281-488-8806 x144

HR - Lockheed Martin:
800-688-8606 x32033
720-568-32033
fax: 303-662-8770

HR - PAE:
800-688-8606 x32078
720-568-2078
fax: 303-662-8770

HR - UTMB:
409-772-8699

Contents	Document #
Changes in 2016-2017	TL-GDE-0005
USAP Deployment Information	TL-GDE-0007
Customs and Immigration	TL-GDE-0009
Baggage Allowance	TL-GDE-0010
Airline Industry Changes	TL-GDE-0017
Computer Requirements for Connecting to the USAP Network	IS-FRM-0012
Deployment Requirements for Information Security Awareness Training	IS-ATT-0001
Acknowledgement of Information Security Policies & Permission for Use*	ICT-FRM_5000.24a
Acknowledgement of USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information*	ICT-FRM_5000.24b
Trip Details*	TL-FRM-0090
Passport Details*	TL-FRM-0097
ECW Sizes* and ECW Gear	TL-FRM-0089
Antarctic Lodging Request Worksheet*	TL-FRM-0092
Business Class Upgrade	TL-GDE-0002

***Please complete and mail to:**

ASC Travel
7400 S. Tucson Way
Centennial, CO 80112-3938
or fax to 303-705-0742

1) Acknowledgement of Information Security Policies & Permission for Use (ICT-FRM_5000.24a)
2) Acknowledgement of USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information (ICT-FRM_5000.24b)
3) Trip Details (TL-FRM-0090)
4) Passport Details (TL-FRM-0097)
5) ECW Sizes (TL-FRM-0089)
6) Antarctic Lodging Request Worksheet (TL-FRM-0092)
7) Permanent, fulltime employees please submit a Fulltime Deployment TRW (TL-FRM-0095) instead of a Trip Details.

USAP records are maintained in accordance with NSF Privacy Act Regulations.

Photo Credit: Deven Stross

CHANGES IN 2016-2017 for ASC PERSONNEL

Baggage Allowance to McMurdo, South Pole

The baggage allowance on the Ice flight between Christchurch and McMurdo is now 85 pounds (38.5 kg), plus carry on, for all participants. There is no longer a distinction between summer and winter participants. Still strictly enforced in both directions.

Prat Pier Security Card

In Punta Arenas, USAP participants must now present a “QR code card” with their passport to gain access to the warehouse and pier. Damco will distribute this card to each passenger upon arrival.

Commercial Travel Blackout Dates Nov 28 - Jan 2

Due to the high cost of travel during the holidays, commercial travel blackout dates this season are November 28, 2016 through January 2, 2017. Commercial travel blackout dates apply to Actual Date redeployments northbound from Christchurch and Punta Arenas. FAA redeployments are not affected.

USAP DEPLOYMENT INFORMATION
for ASC Employees

- Please direct job-specific questions to your Hiring Manager.
- Passports must be valid for six months *after* your return; undamaged beyond normal wear and tear, with a blank page for each country to be visited. Please take the time to check it now. Airline carriers will not allow you to board at your AOD, and some countries will not allow entry, if these requirements are not met.
- Check the expiration of your ATM and credit cards, too, before you deploy. Palmer Station is cashless.
- Fill out and return the forms in this packet by fax or U.S. mail at least eight weeks before your scheduled deployment date. (Alternates too, please.) You do not have to wait until you PQ. Blank forms are available at http://www.usap.gov/travelAndDeployment/contentHandler.cfm?id=765. Please do not return forms via email; fax and U.S. mail are more secure.
- Be sure ASC has your current contact info! ASC uses the email and mailing address you give us on your travel forms. Let ASC Travel know if your situation changes. Also:
  - The name on your ticket *must* match your passport and if it does not, the airlines will stop you at check-in. "Name exactly as it appears on passport" means exactly that.
  - The Airport of Departure is the airport closest to your home address. If you wish to depart from another city, your ticket is roundtrip and you'll be returned to that same location.
- You must submit your HR and travel paperwork and be PQ'd before tickets can be purchased. Late submittal might jeopardize your deployment or even your employment.
- Keep copies of your travel forms in case anything is lost in transit.
- Your Ice dates are determined by your job and your supervisor. Changes are coordinated through your Hiring Manager. Be prepared to travel on weekends and maybe holidays. ASC Travel is unable to change your Ice dates so please do not ask them.
- Orientation for McMurdo and South Pole is partly in Christchurch, partly on the Ice. There isn't a lot of free time in Christchurch. Orientation for Palmer and vessels is in Denver.
- All travel arrangements are made in accordance with the Federal Acquisition Regulations (FAR) and in the best interest of the U.S. Government. Contract employees are not allowed pre-deployment personal travel en route to Antarctica. Please do not ask ASC Travel to consider special routing or layovers, which can be considered misuse of government funds.
- Though QANTAS and American Airlines service the Los Angeles - Auckland route again, the number of seats via Auckland is limited. ASC Travel will book both routes, driven by programmatic availability.
- Review your airline's baggage policies before departure and be prepared to pay baggage fees if the first leg of your travel is not on American Airlines. The USAP allows two normal-size 50lb/23kg checked bags on commercial flights to New Zealand and Chile. If you travel within these allowances and are still charged baggage fees, you may expense them back to your ASC teammate *with receipts*. However, charges for oversize bags (for example, hockey or ski bags) are not reimbursable.
- USAP baggage allowances do not apply to personal or leisure travel. If you elect anything other than FAA during redeployment, you are responsible for all airline baggage fees.

- For the Ice flight between Christchurch and McMurdo, the baggage allowance is 85lb/38.5kg for all participants, strictly enforced. (Save room for about 10lbs of extra ECW gear.) The number of bags is not limited but the maximum weight for a single piece is 70lb/32kg. Hand carry is limited to 15 pounds that must fit into a standard airline sizing box.

  On board the vessels, there are no weight restrictions but space is limited.

- Some airlines charge for preferred seating and special meals. ASC Travel tries to honor your preferences but cannot pre-pay or reimburse airline surcharges. Most seats on international flights aren't assigned until check-in.
- Travel documents are emailed after you return the forms in this packet, about a month before deployment. These include a 12-month visa for New Zealand or a USAP participation letter for Chile, but *not* your ticket which is emailed separately.
- Tickets are e-tickets. Your final itinerary is emailed 14-21 days before deployment; you'll want to print it and bring it with you. Please check your email (including SPAM folders) frequently as deployment approaches.
- Once you're ticketed, the Christchurch office emails the details of your hotel reservation and ECW issue. For those of you going to South America, those details are provided when you arrive in Punta Arenas. Room and taxes in Christchurch and Punta Arenas are direct billed to ASC but the hotel will swipe a personal credit card for incidentals.
- Package mail to the Ice is limited after Thanksgiving, so holiday packages should be mailed via U.S. Mail no later than October 15th. (Tell your friends and families, too.) Even so, there are no guarantees with package deliveries. First Class mail is *not* restricted so it might be wisest to mail essential items to the Ice as First Class flat/envelope mail.
- For other information about life on the Ice, consult the online *USAP Participant Guide*. For example:
  - Bring (extra) sunglasses.
  - Bed linens are provided but not towels.
  - No skyping, no drones.
  - Bring your own long underwear.
- Any TDY in Christchurch must be pre-approved.
- If there are changes to your medical or dental health after you PQ, you *must* notify medical@usap.gov before you deploy.
- All wintering females of child-bearing age are screened for pregnancy one to two weeks before station close. Pregnancy is a "Not Physically Qualified" condition for Antarctic deployment.
- Redeployments are processed from the Ice and are coordinated with your supervisor or MPC.

ASC Travel
7400 South Tucson Way
Centennial, CO 80112

phone: 800-688-8606 x33202 or 303-790-8606 x33202
fax: 303-705-0742

CUSTOMS AND IMMIGRATION

PASSPORTs

Regardless of nationality, your passport must be valid for six months *after* your return.

VISAs – U.S.Citizens

If you are a U.S. citizen you do not need a visa for New Zealand, Chile, or while transiting through Australia.

VISAs – non U.S.Citizens

If you do not possess a U.S. passport, the U.S. Antarctic Program does not pay for, or provide advice about, obtaining visas. Any necessary visas should be obtained *at least eight weeks before deployment* by contacting the embassy of the countries to be visited. **Failure to do so could delay or even prevent your deployment.**

For Australia and New Zealand, request a visitor's visa.

For Chile, request a multiple-entry tourist visa. As far as Customs and Immigration is concerned, you will be entering and departing Chile twice.

If you need a letter identifying you as a USAP participant in order to obtain a visa, please contact ASC Travel.

New Zealand

All participants receive a letter that identifies them as a USAP participant, to whom New Zealand grants an extended visitor visa valid for 12 months. The 12 months start the day you arrive in New Zealand and Ice time is included in your New Zealand "trip."

If you plan on traveling in New Zealand after your deployment, you must not let your visitor visa expire. Electronic visa extensions are available for up to three months by emailing INZCHCHExpress@mbie.govt.nz before you leave the Ice. Visas can also be extended in person at any NZ Immigration office, for a fee.

There is no longer a 14-day grace period in New Zealand if your visitor visa expires while deployed. If you're deploying longer than 12 months, you'll need to email INZCHCHExpress@mbie.govt.nz and obtain a three-month extension *before* you leave the Ice.

When you stay in New Zealand as a tourist, the U.S. Antarctic Program is no longer your sponsor, and you are responsible for observing Immigration and Customs regulations.

High Value Goods

If you plan on carrying any single item worth more than US $1000, excluding personal items such as laptops and cameras, please indicate that on the *Trip Details* form in this packet.

Tobacco Products

You are entitled to bring the following quantities of tobacco into New Zealand duty-free. Anything more is subject to Customs duty and goods and services tax (GST). These restrictions do not apply to electronic cigarettes.

- 50 cigarettes, or
- 50 grams of cigars or loose tobacco, or
- A mixture of all three weighing not more than 50 grams.

Websites

New Zealand Customs home page: www.customs.govt.nz
Visas: http://www.customs.govt.nz/inprivate/traveltonz/immigration/Pages/default.aspx
Duties and allowances: www.customs.govt.nz/features/charges
Prohibited and restricted items: http://www.customs.govt.nz/features/prohibited/imports/Pages/default.aspx

Chile

U.S. citizens with a valid passport can enter Chile for up to 90 days on a tourist visa, reset at each port of entry.

Websites

Visas (unofficial): http://chile.travisa.com/Common/TVSVisaInstructions.aspx?countryid=cl
FAQs: www.aduana.cl/frequently-asked-questions-international-travelers/aduana_eng/2013-04-15/142533.html

Australia

U.S. citizens transiting through Sydney do not need a visa, however, you must stay inside the transfer area of the international terminal. "Transiting" is defined as changing flights/traveling through the airport for less than eight hours. Leaving the terminal is a violation of Australian law.

A scheduled layover in Sydney longer than eight hours requires an electronic visitor's visa (ETA subclass 601). Passengers with ETAs *are* allowed to leave the terminal. If ASC Travel purchases your ticket and your passport is ETA-eligible, an ETA will be purchased about a week before your deployment and attached electronically to your passport. Participants from ETA-ineligible countries should apply for a visitor's visa at least eight weeks before deployment. If you are self-ticketing, you'll need to purchase the visa yourself.

When unscheduled flight delays create a layover longer than eight hours, the airline generates an ETA for you before you land. If you are delayed through your own fault, be prepared to purchase the ETA yourself.

Sea travel requires a Maritime Crew Visa as well (MCV Class 988). If you're boarding a ship in Hobart, the MCV must be obtained before you arrive in Australia, and the application can take up to 30 days. ASC Travel can assist.

Websites

Australian Customs home page: http://www.customs.gov.au/
Visas: http://www.border.gov.au/Trav/Visa
Electronic Visitor's Visa (ETA Class 601): http://www.border.gov.au/Trav/Visa-1/601-
Maritime visas (MCV Class 988): http://www.border.gov.au/Trav/Visa-1/988-
Duties and allowances: http://www.border.gov.au/Trav/Ente/Duty-Free-concessions
Prohibited and restricted items: http://www.border.gov.au/Busi/Impo/Proh

United States

ESTA

IF you do **not** possess a U.S. passport, ***and***:

- IF your travel originates in a foreign country (excluding Canada), ***and***
- IF you are transiting through the U.S. en route to Antarctica,

you must register with ESTA (Electronic System for Travel Authorization) at https://esta.cbp.dhs.gov/esta/ before you leave home. This is a requirement of the U.S. Department of Homeland Security and applies even if you are only in the U.S. to connect to another flight.

From the U.S. Customs and Border Protection website:

> "If a traveler is only planning to transit through the United States en route to another country, when he or she completes the ESTA application, the traveler should enter the words "In Transit" and his or her final destination in the address lines under the heading 'Address While In The United States.'"

ASC Travel
7400 South Tucson Way
Centennial, CO 80112
800-688-8606 x33202 or 303-790-8606 x33202

Information on this page is subject to change.

BAGGAGE ALLOWANCE

Check your airline's baggage policies before departure and be prepared to pay fees at the counter. ASC will reimburse within the baggage allowance *with receipts*.

Ice flight allowances are strictly enforced; excess baggage must be pre-approved.

McMURDO/SOUTH POLE

SUMMER participants

COMMERCIAL FLIGHTS to Christchurch
2 BAGS*
50 lbs (23kg) each
+ carry on**

ICE FLIGHT
85 lbs (38.5kg)
+ carry on**
(save room for 10 lbs of ECW gear)

WINTER participants

COMMERCIAL FLIGHTS to Christchurch
2 BAGS*
50 lbs (23kg) each
+ carry on**

ICE FLIGHT
85 lbs (38.5kg)
+ carry on**
(save room for 10 lbs of ECW gear)

PALMER/VESSELS

all participants

COMMERCIAL FLIGHTS to Punta Arenas
2 BAGS*
50 lbs (23kg) each
+ carry on**

ON BOARD
no weight restrictions but space is limited

There are weight and balance concerns on all flights to the Ice. The USAP reserves the right to bump personal baggage in order to meet safety and cargo requirements.

★ NO AIRLINE ACCEPTS BAGS OVER 70 LBS ★

Note: The USAP baggage allowance does not apply to personal travel. If you elect anything other than FAA when redeploying, you are responsible for all baggage fees.

*no oversize bags such as hockey or ski bags

**must fit into a standard airline sizing box

AIRLINE INDUSTRY CHANGES

Airline policies are beyond ASC's control.

Limited Baggage Transfers:	*Ask when you check in*: How far are your bags going? Increasingly, airlines are not honoring baggage transfers between carriers	You might have to retrieve your bags and re-check them at Los Angeles, Dallas or Miami, especially if you switch airlines en route. ASK when you check in.
Number of bags:	See the *Baggage Allowance* page.	Be prepared to pay baggage fees at the counter, especially if the first leg of your flight is not on American Airlines.
Check-in:	90 minutes domestic, 2 hours international.	Later than that, the airline can deny boarding.
Special Meals:	Airlines often charge for special meals.	ASC will submit your request but cannot reimburse airline surcharges.
Seat Preference:	Airlines often charge for preferred seating.	Seat assignment on international flights is often delayed until check-in. ASC will submit your preference but cannot guarantee aisle or window seating.
Passports:	Valid six months *after* return Undamaged beyond normal wear and tear At least one blank page for every country you plan on visiting	If not, the airline can deny boarding at your AOD.
ID:	Name on your government-issued ID (i.e., passport) must match the name on your ticket *exactly.*	If not, you WILL be denied boarding at your AOD.
Homeland Security:	Last minute changes; no-shows.	Raises red flags, incurs delays at check-in. If you skip, miss, or change any flight leg, notify ASC Travel.

Confirm your itinerary with the airline(s) 24 hours prior to flight.

Last minute changes are difficult, if not impossible to accommodate.

Don't miss your flight! ASC may not be able to rebook you.

United States Antarctic Program

Computer Requirements for Connecting to the USAP Network

The United States Antarctic Program (USAP) addresses US federal government security and operational requirements for computing systems by screening *all* computers (including scientific/research instrumentation systems, mission operation systems, workstations, personal computers (PCs), servers, laptops, and portable notebooks) prior to connecting to the USAP network.

The following system requirements and operating system specifications apply to *all* computing devices — including laptops, smart phones, tablet devices, and Personal Digital Assistance (PDA) — that could connect to the USAP network.

The latest information regarding USAP computer requirements, service, and infrastructure can also be found at http://www.usap.gov/usapgov/technology/index.cfm?m=4. Please direct inquiries to the USAP Help Desk at (720) 568-2001 or helpdesk@usap.gov.

> To minimize wait time for computer screening, please ensure that your system meets the requirements identified in this document prior to deployment. Failure to comply with these guidelines may result in excessive delays or a denial of access.

A computer system must continuously maintain compliance with these computer requirements. A system that falls out of compliance (e.g., falls behind with anti-virus definitions, patches, or vulnerability remediation) may be disconnected without notice if the NSF determines there is an unacceptable level of risk or threat to the USAP environment.

System Requirements

Operating System and Software Patches

Devices running an operating system (OS) must be running at a version currently supported by the vendor and be updated with the most current patch level of the OS, including the most recent security patches. Applications running on the system must also be patched when patches are released by the software vendor.

Antivirus

All devices must have antivirus software running at the current version, and must be configured for automatic updates. Computers must be free of viruses prior to connecting to the USAP network and must maintain the current DAT version as updates are available.

Connectivity

Participants must provide all necessary equipment to connect the computer system to the USAP network, including the Network Interface Card (NIC), external dongles or attachments used by the NIC, device drivers, etc. All equipment must be in working order.

Prohibited Protocols

Telnet and FTP are prohibited, as they present a high risk to the USAP network. These protocols must be replaced with secure versions such as SSH and SFTP.

Client and Server Software

Permitted for use are client software used for the purposes of email and web browsing as well as other client software, such as SSH and SFTP. Software that is not permitted for use on the USAP network includes but is not limited to the following:

- Peer-to-peer (P2P) software (e.g., BitTorrent, KaZaA, Gnutella, Freenet)
- Email server software that provides SMTP/POP port services; some examples include Exchange, Eudora, and send mail.
- Web server software that provides HTTP/HTTPS/FTP services; some examples include IIS, Apache, and Lightppd.
- Network management servers, such as DNS and SNMP.
- Network or port scanning software, such as Nessus.
- Network penetration tools such as Metasploit, BackTrack, and Wireshark.
- Unauthorized wireless access points and other network devices (e.g., firewalls, routers, etc.)

Software requiring NSF approval for use on the USAP network for official business purposes (such as educational outreach) includes Skype and other network bandwidth intensive applications, including video and audio streaming software.

Computer Screening Process

Screening technicians gather the information in the following table during the computer screening process. System operators who connect to the USAP network without a screening rating of “Pass” are in violation of USAP information security policy and may be disconnected without notice. A “Fail” rating indicates that the system owner is responsible for remediating the system as soon as possible to remain connected to the USAP network.

Data Collected By Computer Screening	
Owner’s full name	All MAC addresses
Agency	OS version and patch level
Computer make and model	Antivirus software version and DAT file date
Computer hostname	Technician’s name

United States Antarctic Program

Deployment Requirements for Information Security and Privacy Training

This document outlines information regarding information security awareness training requirements for all United States Antarctic Program (USAP) participants and provides instructions for meeting those requirements. For more information, refer to the parent document, *Information Security Awareness Training* (IS-SOP-9106).

Information Security Training Acknowledgment Requirement

The National Science Foundation (NSF) has mandated that prior to gaining access to the USAP network and network resources (including accessing the Internet from a USAP location), all USAP participants are required to perform the following:

- Complete Information Security and Privacy Training course online.
- Sign and return the *Acknowledgement of Information Security Policies and Permission for Use* form
- Sign and return the *Acknowledgement of USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information* form.

These actions are required annually. These mandates stem from the *Federal Information System Management Act of 2002* (FISMA), and are required as a condition for deployment. USAP Information Security policies and Enterprise Rules of Behavior (EntRob) can be found at http://www.usap.gov/technology/contentHandler.cfm?id=1563

You will not be granted any USAP Network access (including access to the Internet) if you have not completed these requirements.

ASC employees are required to complete Information Security and Privacy Training prior to deployment, during orientation. Instructions for completing this training may also be provided by your Human Resources department. We strongly encourage completing this requirement prior to deployment to Christchurch, NZ or Punta Arenas, Chile.

Instructions for Creating an Online Learning Center (OLC) Account and Completing Assigned Training

Note Returning ASC participants already have a USAP OLC account. Do not create a new account. If unsure of your username or password, email Denver.helpdesk@usap.gov.

1. Visit the USAP Online Learning Center page [http://www.usap.gov/onlinelearningcenter/] for a basic overview of the training system.
2. Click Enter USAP Online Learning Center to be taken to the training site.
3. Click Sign Up on the right side of the Login box.
4. The New User Account form appears. Complete the form by entering all required fields. Also:
   - Make a note of your username and password. You will need this information to log in once you complete the account creation process.
   - Create a password that is at least 12 characters long. The password *must* use at least three of the following four character sets: Uppercase letters, lowercase letters, numbers, and special characters.

- Enter the Course Access Code: **91nbe1a3**.
- Select the correct Participant Organization. This determines the courses assigned to you. If unsure which Participant Organization to select, check with your USAP deployment contact.
- **ASC Employees** (including PAE, GSC, and LM): Select "ASC Contract" for seasonal employees or "ASC Full Time" for full-time employees in the Participant Organization field. Include the name of your employer in the Teammate field.

5. You should receive an email confirming the account request, and then another granting you approval to access the site. After receiving the second email, login using the username and password you created.
   - If you do not receive either of these emails and are unable to log in, please contact the ASC Denver Help Desk at Denver.HelpDesk@usap.gov.
6. Logging in takes you to the Learning Plans page. To access the Information Security and Privacy Training course, click on Courses in the left pane. Click the Launch button to access the Information Security and Privacy Training course.

Note To return to this page at any time, click the My Training tab at the top of the page and then click Learning Plans at the bottom right of the page.

7. The Course Launch page appears. Click Launch link under the Course Modules heading to launch the course materials in a new window.
8. Click Next on each slide and read through all course material.
9. Upon completing the course, close the Course Module window and wait for the Course Launch page to refresh.
10. Click Download to access and/or print your completion certificate.
11. Verify that your name is correct. If correct, you are now recorded in the USAP Online Learning Center as having completed Information Security and Privacy Training course.

Note Depending on the browser used, your name may not appear. Your name should become visible once you save and open or print your certificate.

12. Save an electronic version of the certificate in a personal folder, or print and keep it as proof you completed this requirement.
13. Fill out and sign the *Acknowledgement of Information Security Policies and Permission for Use* form and the *Acknowledgement of USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information*, both of which are included in your deployment packet.

Note Electronic signatures are not accepted at this time.

14. Return the completed forms (5 pages) to the following address:

    ASC Travel
    7400 S. Tucson Way
    Centennial, CO 80112-0742
    or fax to 303-705-0742

For questions or issues in accessing the Online Learning Center, or if you encounter problems with the OLC website or while taking the course, contact the ASC Denver IT&C Help Desk, at 1-800-688-8606, extension 32001, or email Denver.HelpDesk@usap.gov.

The National Science Foundation
Polar Programs
United States Antarctic Program

Acknowledgement of Information Security Policies & Permission for Use of National Science Foundation/United States Antarctic Program Information Systems and Services
ICT_FRM_5000.24a

Document Release History

Release Number	Release Date	Description of Changes	Changes Made By	Organization
1.0	10/20/2014	Initial release as USAP form	Patrick Smith	NSF

1 SCOPE OF AUTHORIZATION

Permission for use of National Science Foundation/United States Antarctic Program (NSF/USAP) information systems and services is restricted to authorized participants in the United States Antarctic Program, designated contractors and U.S. Government employees, official visitors, or individuals otherwise having an authorized purpose for gaining access to, and utilizing the services of, NSF/USAP owned, operated, or provided information systems and services. USAP information systems and services include, but are not limited to, those located at the Denver, CO; Charleston, SC; Arlington, VA operating locations and at USAP facilities in Port Hueneme, CA; Christchurch, NZ; Punta Arenas, Chile; Antarctic stations and research vessels.

2 AGREEMENT PROVISIONS

Permission for use of NSF/USAP information systems and services requires the following acknowledgements:

1. Government owned system. The information systems of the United States Antarctic Program are National Science Foundation federal government owned information systems. When attaching or otherwise interconnecting personally or privately owned information systems with government systems, the NSF reserves the right to extend its information security policies, Rules of Behavior, procedures, and guidance to these systems in order to ensure the integrity of NSF/USAP systems.

2. Mandatory awareness training. Individuals using NSF/USAP information systems and services must receive information security awareness training no less than once annually. Awareness training is a prerequisite for gaining permission to use NSF/USAP information systems and services. Permission to use NSF/USAP information systems and services may be suspended, revoked or denied, as appropriate, for individuals who have not fulfilled the mandatory awareness training requirement.

3. Only authorized use is permitted. Individuals using NSF/USAP information systems and services without authority, or in excess of their assigned authority, are subject to revocation of access privileges, in part or in whole. Further, access for purposes beyond authorization or assigned authority may be a violation of federal law. Penalties for misuse may include, but are not limited to, appropriate administrative sanctions, civil liability or criminal prosecution.

4. No expectation of privacy. Individuals using NSF/USAP information systems and services should be aware that they have no expectation of privacy. Files maintained in NSF/USAP information systems, including electronic mail files, may be reviewed by NSF officials who have legitimate reasons to do so when authorized by the Director or Deputy Director, or by the Inspector General. Individuals should be aware that NSF reserves the right to conduct work-related investigations for the purpose of investigating work-related misconduct, such as violations of the acceptable use policy.

5. Common Authority and Consent to be Monitored. In the course of conducting routine and corrective systems maintenance and administration, NSF designated systems technical personnel have legitimate work-related needs for access to files, contents of files, configuration data, and system log information, as well as monitoring of user

_____ / _____
Initials Date

activities. This extends to any personally or privately owned information systems attached to, or otherwise interconnected with, NSF/USAP systems such that the electronic exchange of information between the two is possible. If such work-related activities reveal possible evidence of criminal wrongdoing, NSF authorizes system personnel to provide the information gained from such activity to NSF officials for administrative action, with referral of such matters to law enforcement officials when appropriate.

6. Protection of sensitive information. Individuals granted access to NSF/USAP information systems and services may, in the course of their official duties, have access to information designated by NSF as sensitive, or protected by federal law including, but not limited to, personal information, procurement information, trade secrets, and other information types. Individuals in such circumstances agree that the confidentiality, integrity, and availability of this information must be protected from unauthorized disclosure, loss, or corruption. Individuals found to be in violation of this prohibition may be subject to appropriate administrative sanctions, civil liability or criminal prosecution.

3 LIMIT OF ACCESS AUTHORITY

Permission to access or otherwise utilize NSF/USAP information systems and services shall be terminated upon separation from the United States Antarctic Program to include, but not limited to, termination of grant or grant extensions, termination of employment in support organizations, termination of Government employment, termination of guest/visitor status, determinations by NSF designated authorities to restrict or terminate access, etc. Continued use of NSF/USAP information systems and services, once access authority has terminated is a violation of federal law.

4 ACKNOWLEDGEMENT

I, the undersigned, understand that I am authorized to access NSF/USAP information systems and services, as defined under the provisions of this Agreement. I acknowledge that I have received the required information security awareness briefing and my responsibility to abide by all information security policies, Rules of Behavior, procedures, and guidance issued by the National Science Foundation as applied to the United States Antarctic Program information systems and services, either directly or through its duly designated support organizations. I further acknowledge that I have read and understood the terms of this Agreement and agree to abide by them.

Printed Full Name:	Date:
Signature:	
Organizational Affiliation:	
Sponsoring Organization:	

The National Science Foundation
Polar Programs
United States Antarctic Program

Acknowledgement of United States Antarctic Program Rules of Behavior for Sensitive Information and Personally Identifiable Information
ICT_FRM-5000.24b

1 GENERAL INFORMATION

The purpose of the United States Antarctic Program (USAP) Rules of Behavior for Sensitive Information (SI) and Personally Identifiable Information (PII) is to highlight federal laws and guidelines from NSF and other federal documents for USAP participants with access to SI or PII.

Sensitive Information is information that has been characterized in accord with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* & National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1 rev 1, *Guide to Mapping Information and Information Systems to Security Catagories* as requiring access restrictions and protection from unauthorized disclosure. Basic types include:

- Privacy Act Systems of Records
- Personal medical information (PHI – Protected health information)
- Personal Identifiable Information
- Financial information
- Trade Secrets Act protected data
- Comercial proprietary data
- Operational Security (OPSEC) information
    - Current US Air Force and Air National Guard flight operation details
- IT infrastructure information
    - detailed internal USAP network diagrams
- Information Technology information
    - root or system administrator passwords to systems on the USAP network
    - vulnerability scan results
    - system log files

Personally Identifiable Information. *OMB M-07-16 defines "personally identifiable information" as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of*

_____ / _____
Initials Date

birth, mother's maiden name, etc. PII examples provided by NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* include but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Federal laws and guidelines pertaining to SI and PII include:

- Privacy Act of 1974 (5 U.S.C. § 552a)
- E-Government Act of 2002 (44 U.S.C. 3601 *et seq.*)
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- OMB Memorandum M-06-16, *Protection of Agency Sensitive Information*
- Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. § 3546)

The USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information (SenROB) must be reviewed and signed by USAP participants with access to SI or PII. Signatories accept that they understand and take personal responsibility for the security of sensitive information and personally identifiable information.

The USAP SenROB is founded on the principles described in federal law, and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, and Office of Management and Budget. Therefore the SenROB carries the same responsibility for compliance as the official documents cited above.

2 USER RESPONSIBILITIES

In the course of performing official duties, USAP participants with access to SI or PII are responsible for avoiding inappropriate access or disclosure of SI and PII of any kind and are bound to follow certain methods of storage and transmission for these kinds of data. These rules of behavior detail the responsibilities of and expectations for all individuals with access to SI or PII.

_____/_____
Initials Date

3 RESPONSIBILITY/ACCOUNTABILITY REQUIREMENTS

- Users should only use systems, software, and data for which they have authorization and use them only for official Polar Programs' business.
- Users with access to systems and data that utilize SI or PII must view and access this information only for the purposes for which use of the data is intended.
- Users must protect sensitive information from unauthorized disclosure.
- Users shall not store SI or PII on portable devices such as laptops, tablets, smart phones and USB drives or on remote/home systems unless approved encryption methods are employed.
- Users are prohibited from transmiting SI or PII via plain text e-mail; only approved encryption methods shall be used.
- All records containing SI or PII must be stored on network drives with access limited to those individuals or entities that require access to perform a legitimate job function.
- All removable or transportable media (e.g., paper forms, reports, cassettes, CDs, USB drives, etc.) containing SI or PII must be secured when not in use. Acceptable security measures depend on the circumstances, but may include locked file rooms, desks, cabinets and encryption.
- Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing SI or PII must be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information in accordance with NIST SP 800-88 Rev 1, *Guidelines for Media Sanitization* and USAP Directive 5000.22, *Media Protection Policy*.Organizations must follow their media sanitization procedures.
- In accordance with OMB Memorandum M-07-16, users must immediately report actual and potential incidents of inappropriate disclosure of SI or PII to the USAP Help Desk Toll Free at 1-800-688-8606 (Extension 32001) or (720)-568-2001 within 24 hours of detection.

USAP participants who have access to SI or PII must adhere to these rules and guidelines. I acknowledge receipt of, understand my responsibilities for, and will comply with the USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information.

Signature of User	Date
Printed Name of User	Affiliation

TRIP DETAILS
FOR ASC EMPLOYEES

Date: _____

Return this form to: ASC Travel, 7400 South Tucson Way, Centennial, CO 80112-3938
Fax: 303-705-0742; phone: 800-688-8606 x33202 or 303-688-8606 x33202

NAME: *(last, first, full middle name)*	NICKNAME:	GENDER: ☐ M ☐ F

MAILING ADDRESS:	PERMANENT ADDRESS: (*if different*)	CONTACT INFO: CELL: _____ WORK: _____ HOME: _____ EMAIL(s): _____

Departing from: ☐ Mailing address ☐ Permanent address **AIRPORT OF DEPARTURE:** _____
☐ Other: _____
Physical address required (no P.O. boxes) for mileage reimbursement.

Passport Status:
☐ Valid for six months after deployment ☐ No passport yet ☐ Other: _____

Job Title: Winterover? ☐ Yes ☐ No

Employed by (check one):
☐ Best Recycling ☐ Lockheed Martin ☐ Other: _____
☐ Gana-A-'Yoo (GSC) ☐ PAE
☐ GHG ☐ UTMB

Have you deployed before? ☐ Yes ☐ No What year?

Seating:*	Special Meals:*	Freq Flyer 1: Airline _____ FF # _____
☐ Aisle		Freq Flyer 2: Airline _____ FF # _____
☐ Window		Car Rental: Agency _____ Rewards # _____

Hotel in Christchurch: Hotels in Christchurch are assigned

Hotel in Punta Arenas: *1st choice, not guaranteed*
☐ Cabo de Hornos ☐ Diego de Almagro ☐ Dreams
☐ Jose Nogueria ☐ Isla Rey Jorge ☐ straight to vessel

Hotel Check-In Date: Check-Out Date:

Room Type: ☐ Smoking ☐ Non-Smoking ☐ Single ☐ 2 Twin Beds ☐ 1 Double Bed
Roommate Request: _____
No Hotel Required: ☐ Local contact phone number: _____

**You are responsible for airline surcharges.*

PASSPORT DETAILS

ASC Travel must collect current passport information from all deploying participants for ticketing and visa purposes.

Your passport must be valid for six months after redeployment, undamaged beyond normal wear and tear, with a blank page for each country en route.

Complete and submit form via secure fax 303-705-0742 or U.S. Post Office Mail. **Do *not* email this document.**

Enter information *exactly* as it appears on passport, and please print legibly.

Last Name: _____ **Suffix:** _____

First Name: _____

Middle Name: _____ **no middle name:** ☐

Gender: **Male** ☐ **Female** ☐

Nationality: _____

Passport Number: _____

Date of Birth **Day:** **Month:** **Year:** _____

Country of Birth: _____

Date of Issue **Day:** **Month:** **Year:** _____

Date of Expiration **Day:** **Month:** **Year:** _____

Passport must be good for six (6) months after return.

Issuing Authority: _____

Do you hold any citizenship other than the nationality provided with the passport above? **Yes** ☐ **No** ☐

Redress # (if any):* _____

USAP Records are maintained in accordance with NSF Privacy Act Regulations.

* A Redress Number is a unique 13-digit identifier issued by the Department of Homeland Security to individuals who have applied for a Redress Number through the Traveler Redress Inquiry Program (TRIP). Under the terms of the Secure Flight program, such individuals shall provide their Redress Number when making all travel reservations.

ECW SIZES CLOTHING HAT Boots Gloves

Please print clearly

Your Name: _____

(First name, Full Middle Name, Last Name)

Gender: ☐ Male ☐ Female

Deploying to: ☐ McMurdo ☐ South Pole ☐ remote field camp ☐ Palmer/vessels

Season: ☐ WINFLY ☐ Summer ☐ Winter

You are a (check one):

☐ Grantee ☐ Tech Event ☐ Seasonal Contractor ☐ Fulltime ☐ Other (specify): _____

Event #: _____

☐ Best Recycling
☐ Gana-A'Yoo (GSC)
☐ GHG
☐ Lockheed Martin
☐ PAE
☐ UTMB

☐ NSF Staff

Job Title: _____

Height:		Weight:	
Jacket Size:	☐ x-small ☐ small ☐ medium ☐ large ☐ XL ☐ 2XL ☐ 3XL ☐ 4XL		
Chest Size:			
Knit Hat Size:	☐ x-small ☐ small ☐ medium ☐ large ☐ XL ☐ 2XL		
Glove Size:*	☐ x-small ☐ small ☐ medium ☐ large ☐ XL ☐ 2XL ☐ 3XL		
Waist (inches):		Hip (women):	
Inseam (inches):		Shoe Size:	
Additional Requirements:			

*For gloves, measure around the fullest part of the palm (excluding thumb). Measure from the tip of the middle finger to the base of the hand. The largest measurement is your glove size.

Inches	7	7½-8	8½-9	9½-10	10½-11	11½-12	12-13½
Centimeters	18	20	23	25	28	30	33
Glove Size	XS	S	M	L	XL	2XL	3XL

ECW GEAR

USAP participants must supply their own <u>socks</u> and <u>base layer insulation clothing</u> to fulfill the ECW clothing requirement.

The following ECW clothing items are **<u>required</u>** to deploy to Antarctica, including both the USAP-provided and participant-provided clothing (no changes since 15-16). Ask you supervisor or science implementer if you have questions about appropriate clothing.

USAP-Provided ECW Clothing

- Parka (continental) or windbreaker jacket (peninsula)
- Boots
- Windpant/windbib or insulated Carhartt bib (item issued depends on job duties/work location)
- Fleece/pile insulation layer
- Hat
- Gloves
- Neck gaiter
- Goggles
- Rain jacket and rain pants (peninsula only)

Participant-Provided, and Required, ECW Clothing

The following items must be supplied by the participant.

- Socks
  - Mountaineering, winter-weight, non-cotton
  - Fabric suggestions: Merino wool or nylon/lycra blend
  - An additional, lightweight, liner sock to be worn underneath is suggested to assist in wicking (moving) sweat away from the foot (e.g., merino wool or polypropylene)
  - Suggested quantity is 2-4 pairs each
- Base layer, lightweight (thermal, long underwear - tops and bottoms)*
  - This insulation layer is worn directly next to skin and assists with wicking sweat and moisture away from the body
  - Fabric suggestion: synthetics (e.g., polypropylene, polyester, branded materials) or natural fibers (e.g., silk or merino wool)
  - Non-cotton
  - Density approximately 140-200 grams per square meter
    - The clothing label or website might list this as “140 weight” or another number within this range
- Base layer, mid-weight (thermal, long underwear - tops and bottoms)*
  - This insulation layer can be worn independently or over base layer
  - Helps protect against cold and wick moisture farther from body
  - Non-cotton
  - Fabric suggestions are synthetics (e.g., polyester, nylon, non-bulky fleece, branded materials such as PolarTec) and natural fibers (e.g., merino wool, down)
  - Density approximately 260-320 grams per square meter
    - The clothing label or website might list this as “260 weight” or another number within this range

*A search engine inquiry for light and mid-weight base layers and mountaineering socks will yield recommendations in several price ranges.

Antarctic Lodging Request Worksheet

(Complete for McMurdo, South Pole and Palmer Stations)

Name: ☐ Male ☐ Female

Station: ☐ McMurdo ☐ South Pole ☐ Palmer

Winterover? ☐ Yes ☐ No

To facilitate your housing in Antarctica, the following information is extremely helpful. Please understand that we cannot guarantee a specific roommate/suitemate or room assignment.

Roommate Requested: _____

Suitemate(s) Requested: _____

If known, do you snore? ☐ Yes ☐ No ☐ Unknown

Are you a smoker? ☐ Yes ☐ No

(Note: Smoking is prohibited in dorm rooms. Smoking is permitted in designated outside areas only.)

Note: Housing for McMurdo and South Pole Stations is assigned.

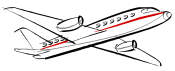
Palmer Station Room or Building Request: ☐ GWR ☐ BIO

Notes / Comments:

If you have any questions or special needs, please contact your USAP Point of Contact.

ASC Travel
7400 S. Tucson Way
Centennial, CO 80112

phone: 800-688-8606 x33202 or 303-790-8606 x33202
fax: 303-705-0742
email: deploy@usap.gov



BUSINESS CLASS UPGRADE

TO/FROM SYDNEY

ASC is able to request an upgrade on your QANTAS flight to/from Sydney to Business Class if you have an American Airlines AAdvantage account with at least 50,000 miles.

Upgrades are optional.

Eligibility:

- You must have at least 50,000 miles in your AAdvantage account and be able to submit proof of your AAdvantage balance.
- You must be traveling on USAP business to/from Christchurch.
- You must be flying AA/QANTAS.
- Your ticket must be purchased by ASC Travel.

Upgrades are issued at the discretion of the airline on a space-available basis upon departure at the boarding gate.

To request an upgrade, wait until you receive your deployment itinerary from BCD Travel, then contact ASC Travel. **Please allow 10 business days for processing.**

ASC Travel
7400 S. Tucson Way
Centennial, CO 80112-3938
1-800-688-8606, x33202
303-790-8606, x33202
303-705-0742 (fax)
deploy@usap.gov

If you are flying another airline or to another destination, such as Punta Arenas, you may upgrade directly with the airline. Be aware, however, that ASC may lose control of the ticket and you risk having no further travel support from ASC or BCD Travel. It may be wisest to upgrade at check-in.