

# DATA SHARING AGREEMENT

between

WASHINGTON DEPARTMENT OF FISH AND WILDLIFE

and

WASHINGTON STATE PARKS AND RECREATION COMMISSION

This Data Sharing Agreement is entered into by and between the Washington Department of Fish and Wildlife (WDFW) and Washington State Parks and Recreation Commission (henceforth RECIPIENT) to establish the content, use, and protection of Washington data needed by RECIPIENT to market the Discover Pass product. This agreement covers such data whether provided by WDFW or collected by RECIPIENT on behalf of WDFW. Data supplied in this agreement is pursuant to Revised Code of Washington; specifically, RCW 39.34 and RCW 42.56.430. This agreement is only for data sharing of the data described below and is a no-cost agreement between the parties.

## 1.0 Period of Agreement

The term of this Agreement shall be in effect from 01/01/2016 to 06/30/2017. This agreement may be extended by consent and signature of both parties and may be terminated in writing by either party.

## 2.0 Intended Use of Data

The RECIPIENT agrees to use the data provided by WDFW under the terms of this agreement for the purpose of Discover Pass marketing.

### 2.1 Description of Data:

WDFW shall provide Discover Pass sales data from the WILD system as contained in FILE LAYOUT, Attachment A. WDFW reserves the right to edit, add, delete or change any data field contained in the FILE LAYOUT as WDFW considers necessary to the functions of WDFW or as applicable to comply with federal and state laws. WDFW will send advance notice to RECIPIENT with the schedule and explanation of changes.

Where both mailing and physical address are provided, only the mailing address will be disclosed in response to request for disclosure from courts, law enforcement agencies, or government entities with enforcement, investigative, or taxing authority and only for use in the normal course of conducting their business.

If the WDFW-supplied data is used for any other purpose other than authorized under this agreement, further access to any WDFW data will be denied, and this agreement will be terminated immediately.

### 2.2 Constraints on Use of Data

The data supplied under this agreement by WDFW to RECIPIENT is the property of WDFW and shall not be shared with third parties without the written permission of WDFW.

RECIPIENT shall protect all data collected, used, or acquired in connection with this Data Sharing Agreement against unauthorized use, disclosure, modification or loss. RECIPIENT shall ensure that its directors, officers, employees, subcontractors or agents use such data only for the purposes of accomplishing the services set forth in this Data Sharing Agreement. RECIPIENT and its subcontractors agree not to release, divulge, publish, transfer, sell or otherwise make all or any part of this data known to unauthorized persons without the express written consent of WDFW or as authorized by law.

**3.0 Data Security**

RECIPIENT shall meet or exceed industry best practices for physical security, data security, network security, and access controls, both technically and procedurally, to protect WDFW data from unauthorized physical and electronic access and to ensure the confidentiality, availability and integrity of all data shared. Upon request, RECIPIENT will furnish WDFW with written documentation of how the requirements of this section will be met. Methods employed are subject to annual review and approval by WDFW and must meet or exceed OCIO Standard 141.10.

**3.1 Data Classification Declaration: Category marked is the data described in this agreement:**

**Category 1 – Public Information:** Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

**Category 2 – Sensitive Information:** Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

**Category 2P – Sensitive Resource Information Subject to WDFW POL-5210:** WDFW policy POL-5210 identifies the specific fish and wildlife data that are exempt from public disclosure, the conditions under which the data can be released, and to whom they can be released.

**Category 3 – Confidential Information:** Information that is specifically protected from disclosure by law. It may include but is not limited to:

- a. Personal information about individuals, regardless of how that information is obtained.
- b. Information concerning employee personnel records.
- c. Information regarding IT infrastructure and security of computer and telecommunications systems.

**Category 4 – Confidential Information Requiring Special Handling:** information that is specifically protected from disclosure by law and for which:

- a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.

b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

**3.2 Data Handling Requirements**

Data handling requirements may vary depending on the classification of data shared with RECIPIENT. The WDFW data shared with RECIPIENT may involve a mix of data classes including sensitive and confidential information. Therefore, whenever data elements are aggregated for collection, transmission, or storage, the aggregate data shall be handled using the protocols that apply to the most sensitive data element.

**3.3 Data Storage**

Regardless of the media employed (e.g., disk, tape, or other media), sensitive and confidential data must be stored in an encrypted format. Documents generated in printed form will be properly secured, disposed, destroyed or shredded when no longer needed so unauthorized individuals cannot collect client information. Data destroyed shall include all copies of any data sets in possession after the data has been used for the purpose as specified herein. If data is not destroyed on site, RECIPIENT must use a secure method or vendor to ensure the destruction is completed as outlined above.

Storage of Category 3 or higher information (see section 3.1 above) on portable or removable media or devices requires that the data be encrypted by a process that uses cryptographic modules validated by the National Institute of Standards and Technology (NIST).

**3.4 Data Transmission**

Per state of Washington IT Security Standard 141.10, transmission of Category 3 or higher information outside of the state government network requires encryption such that: (a) all manipulations or transmissions of data during the exchange are secure; (b) if intercepted during transmission, the data cannot be deciphered; and (c) agencies must use industry standard algorithms, or cryptographic modules validated by the National Institute of Standards and Technology (NIST).

**3.5 Data Protection**

Client systems accessing sensitive information supplied by WDFW under this Agreement must be protected by an anti-malware solution that is automatically updated. Additionally, the client system shall be protected by a firewall to help prevent unauthorized intrusions.

**3.6 Data Backups**

Data backups of confidential information supplied under this Agreement shall be backed up by the RECIPIENT using industry standard encryption modules validated by the National Institute of Standards and Technology (NIST).

**3.7 Data Shared with Subcontractors**

If WDFW data provided under this Data Sharing Agreement is to be shared with a subcontractor, the contractor with the subcontractor must include all of the data security provisions within this Agreement and within any amendments, attachments, or exhibits within this Agreement. If the RECIPIENT cannot protect the data as articulated under this

Data Sharing Agreement, then the contract with the subcontractor must be submitted to the WDFW Contact specified for this Agreement for review and approval.

#### **4.0 RECIPIENT Personnel**

##### **4.1 Access to Data**

RECIPIENT shall limit access to WDFW sensitive and confidential data to those staff members with a well-defined business need. Data will be protected from unauthorized physical and electronic access. Data will be protected in a manner that prevents unauthorized persons from retrieving data by computer, remote terminal or other means.

##### **4.2 Security Training**

RECIPIENT shall provide periodic training to staff on RECIPIENT's internal data security policies and procedures, and on applicable state and federal legal requirements for protecting sensitive and confidential data.

##### **4.3 Prohibition on Mobile Devices and Removable Media**

By signature of this Agreement, RECIPIENT certifies it has a strictly enforced written policy prohibiting the transfer or storage of unencrypted personally identifiable information on mobile devices or removable storage media for any reason.

##### **5.0 Compliance with Applicable Laws and Regulations**

RECIPIENT shall comply with all applicable federal laws and regulations protecting the privacy of personal information.

##### **6.0 Security Breaches**

The Washington Personal Information Notice of Security Breaches (RCW 19.255.010 and 42.56.590) delineates notification requirements in the event of a breach in the security of personal information. RECIPIENT agrees that in the event of any breach or compromise of the security, confidentiality or integrity of computerized data where personal information of a WDFW licensed hunter or angler was, or is reasonably believed to have been, acquired and/or accessed by an unauthorized person, RECIPIENT shall notify WDFW of the breach of the security system containing such data within 24 hours, comply with all notification actions, and/or assist WDFW with all notification actions required by WDFW policy and the law.

If RECIPIENT has reason to believe that personal information transmitted pursuant to this Data Sharing Agreement may have been accessed or disclosed without proper authorization and contrary to the terms of this Data Sharing Agreement, RECIPIENT will, as soon as is practical, give WDFW notice and take actions to eliminate the cause of the breach. To the extent WDFW deems warranted, in its sole discretion but following consultation with RECIPIENT, WDFW will provide notice to individuals whose personal information may have been improperly accessed or disclosed. RECIPIENT shall bear the full costs of such notice to impacted individuals, including any costs incurred by WDFW necessary to meet the requirements of RCW 42.56.590 and/or RCW 19.255.10 and, if reasonably necessary, the costs to retain an outside consulting firm to undertake this effort.

## 7.0 Indemnification

To the fullest extent permitted by law, RECIPIENT shall defend, indemnify, release, and hold WDFW harmless from and against all claims, losses, and expenses against WDFW arising from or pertaining to the performance of this Data Sharing Agreement, the release by any of RECIPIENT employees or agents of such information provided by WDFW, breach of this Agreement, or the violation of any state or federal law applicable to the use, disclosure or protection of data subject to this Agreement.

## 8.0 Amendments and Alterations to this Agreement

This Data Sharing Agreement constitutes the entire agreement between WDFW and RECIPIENT and no other statements or representations, written or oral, shall be deemed to exist or to bind the parties. WDFW and RECIPIENT may amend this agreement at any time, provided that the amendment is in writing and signed by authorized persons.

## 9.0 Termination of Services

In the event WDFW or RECIPIENT terminates this agreement, or RECIPIENT ceases operation, this Data Sharing Agreement shall continue in full force and effect as to any data already transmitted by WDFW to RECIPIENT pursuant to this Data Sharing Agreement.

### 9.1 Destruction of Sensitive Data

Upon termination of this Agreement, RECIPIENT shall ensure that all data supplied by WDFW as described herein is removed and destroyed in a secure manner.

Data received under this agreement will be removed from computer equipment after it has been used for its stated purposes by using a utility for securely overwriting the data from electronic storage media, degaussing the media, or physically destroying the media in such a way that data cannot be recovered. RECIPIENT shall certify in writing within ten business days that all copies of the data stored on RECIPIENT servers, backup servers, backup media, or other media including paper copies have been permanently erased<sup>1</sup> or destroyed.

## 10.0 Dispute Resolution

Except as otherwise provided in this Agreement, should a bona fide dispute arise between WDFW and RECIPIENT that cannot be resolved through discussion and negotiation, either party may request a Dispute Resolution Board. A request for a Dispute Resolution Board must be in writing, state the disputed issues, state the relative positions of WDFW and RECIPIENT and be sent to the other party, which must respond within 10 business days.

Once a party requests a Dispute Resolution Board, each party shall designate a representative. The representatives shall mutually select a third member. The Dispute Resolution Board shall evaluate the facts, agreement terms and applicable statutes and rules and make a determination by majority vote. WDFW and RECIPIENT shall each bear their own costs under this section. The decision shall be admissible in any succeeding judicial or quasi-judicial proceeding concerning the agreement. WDFW and RECIPIENT agree that the Dispute Resolution Board shall precede any action in judicial or quasi-judicial tribunal.

---

<sup>1</sup> "Permanently erased" means the data have been completely overwritten and are unrecoverable. File deletions or media high level formatting operations do not constitute a permanent erasure.

### **11.0 Assignment**

This agreement may not be assigned, in whole or part, by RECIPIENT to any entity without prior written approval of WDFW.

### **12.0 Governing Law and Venue**

This Data Sharing Agreement shall be construed and interpreted in accordance with the laws of the State of Washington, and the venue of any action brought hereunder shall be in the Superior Court for Thurston County, Washington.

### **13.0 Notices**

Any notices made in connection with this agreement shall be in writing and sent certified mail to the following individuals and addresses:

For WDFW:

Matthew Oram  
WILD Systems Manager  
600 Capitol Way N  
Olympia WA 98501  
[matthew.oram@dfw.wa.gov](mailto:matthew.oram@dfw.wa.gov)  
360-902-2626

For RECIPIENT:

Katie Manning  
Business Development Manager  
Post Office Box 42650  
Olympia, WA 98504-2650  
[katie.manning@parks.wa.gov](mailto:katie.manning@parks.wa.gov)  
360-902-8631

### **14.0 Independent Capacity**

The employees or agents of each party who are engaged in the performance of this Data Sharing Agreement shall continue to be employees or agents of that party and shall not be considered for any purpose to be employees or agents of the other party.

### **15.0 Waiver**

A failure by either party to exercise its rights under this Data Sharing Agreement shall not preclude that party from subsequent exercise of such rights and shall not constitute a waiver of any other rights under this Data Sharing Agreement unless stated to be such in a writing signed by an authorized representative of the party and attached to the original Data Sharing Agreement.

### **16.0 Nondiscrimination**

No individual shall be excluded from participation in, denied the benefits of, subjected to discrimination under, or denied employment in the administration of or in connection with any program provided by this Data Sharing Agreement because of race, color, creed, marital status, religion, sex, national origin, Vietnam era or disabled veteran's status, age, the presence of any sensory, mental or physical disability, or political affiliation or belief. Provided that the prohibition against discrimination in employment because of disability shall not apply if the particular disability prevents the individual from performing the essential functions of his or her employment position, even with reasonable accommodation. The parties agree to abide by the standards of responsibility toward the disabled as specified by the Americans with Disabilities Act and applicable Washington state law.

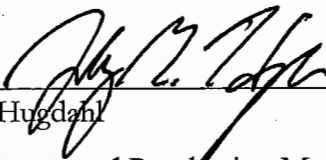
In the event that one of the parties hereto refuses to comply with the above provision, this Data Sharing Agreement may be cancelled, terminated, or suspended in whole or in part by the other party.

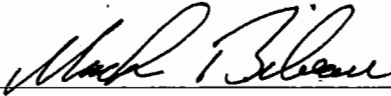
By the signatures of their duly authorized representative below, the Washington Department of Fish and Wildlife, and RECIPIENT, intending to be legally bound, agree to all of the provisions of this Data Sharing Agreement.



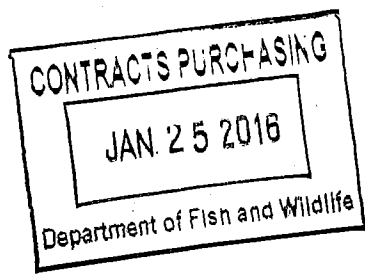
**WASHINGTON DEPARTMENT  
OF FISH AND WILDLIFE**

**WASHINGTON STATE PARKS AND  
RECREATION COMMISSION**

BY:   
Jeff Huggan  
TITLE: Contracts and Purchasing Manager  
DATE: 1/29/16

BY:   
TITLE: CFO  
DATE: 1/15/16

Approved as to form by  
WA Attorney General 01/12/2009



# Attachment A: FILE LAYOUT

[Name of Dataset]

Position	Field Name	Length	Notes:
	CU_First_Name	Text	Customer First Name
	CU_Middle_Name	Text	Customer Middle Name
	CU_Last_Name	Text	Customer Last Name
	CU_Mailing_Street	Text	Customer Mailing Street
	CU_Mailing_Street2	Text	
	CU_Mailing_City	Text	Customer Mailing City
	CU_Mailing_State_Code	Text	Customer Mailing State
	CU_Mailing_zip_code	Text	Customer Mailing Zip
	CU_Mailing_Country	Text	Customer Mailing County
	CU_HOME_Email_Addr	Text	Email
	IT_DESCR	Text	Item Description
	IT_Created_Date	Date	Date Item Sold
	IC_RCN	INT	WILD Item Catalog ID
	LS_Year	Text	License Year of sale
	AG_ID	INT	Agent that sold the item
	AG_Business_County	Text	Agent County
	AG_Business_City	Text	Agent City

WDFW Data Sensitivity Category: 3

Category Approved by



WDFW CIO

Date 12-29-15