

# **P&N Mass Tort Portal Acceptable Use Policy (“AUP”)**

**Postlethwaite & Netterville, APAC**

## **Introduction**

Postlethwaite & Netterville, APAC (“P&N”) provides administrative support services and solutions to the legal industry. P&N often works with its clients and courts to facilitate the collection of confidential information regarding claimants in a specific legal matter. The data collected by P&N is generally obtained from the client, a party to the settlement, the claimant, or an authorized representative of the claimant. P&N utilizes the P&N Mass Tort Portal database (“MTP”), a proprietary database developed and owned by P&N to collect, organize, store, and protect claimant information submitted in connection with Court approved projects for which P&N is engaged. The data stored in MTP may be sensitive, confidential, and/or Personally Identifiable Information (“PII”). P&N is at all times committed to complying with all applicable State and Federal laws governing the collection, use, protection, and destruction of this information. P&N’s AUP and MTP Privacy Notice are designed to help achieve these goals by ensuring that users of MTP take responsibility for the protection and appropriate use of information in accordance with such policies.

By using the MTP, users and entities on whose behalf users are acting (collectively “Users”) agree to comply with this AUP and all such entities shall be responsible for assuring compliance with the AUP by their respective employees, agents, independent contractors and the like. P&N reserves the right to change or modify the terms of this AUP at any time, effective when posted on the MTP website at. Users’ usage of the MTP after changes to this AUP are posted shall constitute acceptance by such Users of any changed or additional terms even if Users have not reviewed the changes.

## **Purpose**

The purpose of this AUP is to provide guidance for the acceptable use of the MTP. Users of the MTP, including P&N employees, independent contractors, and service providers, are granted different levels of access to MTP and datasets within the database depending on their roles within the particular project on which they are assigned. Inappropriate use exposes P&N to risks such as data loss, data corruption, unplanned service outage, unauthorized access to sensitive data, and potential legal issues. As such, all persons who access MTP must agree to the terms set forth in this AUP and P&N’s MTP Privacy Notice.

## Scope of AUP

Use of MTP constitutes Users' acceptance of and agreement to be bound by the terms of this AUP.

## User Accounts and Access Rights

- Users are responsible for the security of data, accounts, and systems under their control, including their credentials for accessing MTP.
- Users shall keep their usernames and passwords secure and shall not share account or password information with anyone.
- Users agree that they will immediately notify the MTP system administrator pursuant to the Incident Reporting and Notification section of this AUP if login, password, or account information becomes compromised or if there is a suspicion that MTP data may have been compromised in any way.
- Providing access to another individual, either deliberately or through failure to secure one's credentials, is a violation of this AUP which can result in the suspension of the right to access or use MTP (See Restrictions on Use section below).
- P&N's authorization to access data within MTP grants Users a limited, non-exclusive, non-transferable, non-assignable, and terminable right to edit, modify, update, and use the data located in MTP in accordance with this AUP and P&N's MTP Privacy Notice solely for the purpose of evaluation/analysis of the data, internal testing, and use in connection with an approved project. Users are granted access only to the datasets applicable to the project on which they are engaged. No access or rights are granted for any other purpose.
- Users should immediately contact the MTP system administrator pursuant to the Incident Reporting and Notification section of this AUP if Users believe that access has been granted to datasets outside of their engagement needs.
- P&N will not ask for your MTP access credentials (username, password, etc.) in an unsolicited phone call, email, or other form of communication.

## Prohibited Uses of MTP

The following activities are prohibited:

- Engaging in activities that are illegal under local, state, federal, or international law.
- Engaging in activities or taking action that is unlawful, harmful to, or in any way interferes with the use of MTP or the data within MTP.
- Unauthorized copying of copyrighted materials including digitization and distribution of photographs from magazines, books, or other copyrighted software for which P&N does not have an active license.
- Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, spyware, ad ware, e-mail bombs, etc.).

- Hacking, attacking, gaining access to, breaching, circumventing, or testing the vulnerability of the user authentication or security of MTP without express authorization of P&N.
- Unauthorized monitoring, scanning, or probing of the network or system or any other action aimed at the unauthorized interception or harvesting of any data contained in MTP.
- Providing guidance, information or assistance with respect to causing damage or security breach to P&N's network or to MTP, or to the network of any other network.
- Revealing MTP access credentials to others or allowing unauthorized use of MTP access credentials by others.
- Effecting security breaches or disruptions of network communications. Security breaches include accessing data of which Users are not an intended recipient or logging into a server or account that Users are not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, degrading the performance, depriving authorized access, disabling or degrading security configurations.
- Unauthorized disclosure of non-anonymized data which breaches the privacy rights of individuals and/or organizations identified within the data by making public PII or PHI other than for the use intended or approved by the supervising court or other authorized client that owns or controls the data.
- Attempting to reverse engineer, decrypt, de-anonymize, derive or otherwise re-identify anonymized information.
- Distributing, disclosing, transferring, or otherwise making available the datasets to any person other than those employed by the same service provider who have also accepted the terms of this AUP and are assisting or collaborating with Users.
- Failing to take reasonable security precautions to help prevent violations of this AUP.

The listed activities are not exhaustive, but illustrate the types of activities which fall into the category of unacceptable use. To the extent Users are unsure whether a particular use is acceptable, Users should contact the MTP system administrator pursuant to the Incident Reporting and Notification section of this AUP for clarification and authorization.

### **Restrictions on Use**

P&N has the authority and reserves the right, in its sole discretion, to refuse or limit access to datasets or discontinue further access and use to Users at any time and for any reason. Users should send a message to the MTP system administrator pursuant to the Incident Reporting and Notification section of this AUP if Users feel that access has been inappropriately denied.

## **Responsibilities of MTP Users**

- Users acknowledge that they have reviewed and understand this AUP and P&N's MTP Privacy Notice which governs the collection, use, disclosure, and destruction of confidential information and PII in MTP.
- By using MTP, Users agree to comply and be bound by the terms of this AUP and P&N's MTP Privacy Notice.
- Users agree that they shall not at any time during their employment, contract, association, or appointment with P&N use information in MTP except as may be required in the course and scope of their duties and responsibilities provided such use is in accordance with applicable law, this AUP, and P&N's MTP Privacy Notice.
- Users agree that they will not use, access, or attempt to access information in MTP after the termination of their employment, contract, association, or appointment with P&N.
- The failure of P&N to insist upon strict compliance with any provision of, or to assert any right under, this AUP shall not be deemed to be a waiver of such provision or right or of any other provision or right under this AUP. Any violation of this AUP or P&N's MTP Privacy Notice, may result in the immediate suspension or termination of Users' access, termination of the service agreement with the service provider, and/or other action entitled by law such as injunctive or equitable relief.
- Users agree that by utilizing MTP, Users' rights and obligations, as well as the rights and obligations of P&N, shall be governed, at P&N's sole discretion, by the laws of the State of Louisiana.
- Users agree that they will notify P&N immediately of any known or suspected violation of this AUP or P&N's MTP Privacy Notice.
- Users understand and agree that their obligations outlined herein will continue even after termination of employment, contract, association, or appointment with P&N.

## **Limitation of Liability**

In no event shall P&N be liable to Users or any third party for any direct, indirect, incidental, consequential, special or punitive damages (including, but not limited to, damages arising from the disallowance of a potential claim against a client of P&N or damages to business reputation, lost business, or lost profits), whether foreseeable or unforeseeable, and however caused, even if P&N is advised of the possibility of such damages, as a result of using MTP and/or the information within MTP. Users have the sole responsibility for the adequate protection and backup of data and equipment used in connection with MTP and Users will not make a claim against P&N for lost data, re-run time, inaccurate output, work delays, or lost profits resulting from the use of materials provided on MTP. All Users agree to hold P&N harmless from, and agree not to sue P&N for, any claims based on or related to the use of MTP.

## **Incident Reporting and Notification**

Users shall notify the MTP system administrator at [dmire@pncpa.com](mailto:dmire@pncpa.com) of all relevant details if:

- Logon or account information is compromise.
- Confidentiality or privacy of data is or is believed to be compromised.
- Users receive any legal, investigatory, or other government demand to reverse engineer, decrypt, de-anonymize, or disclose any data in MTP.
- Access has been granted to datasets outside of their engagement needs.
- Users are unsure whether a particular use is acceptable under this AUP.
- Users access has been improperly denied.

Any notification that P&N sends to its Users pursuant to this AUP will be sent via e-mail to the e-mail address on file with P&N, or may be in writing to Users addresses of record. It is the responsibility of the Users to promptly notify P&N of any change of contact information.

**By using MTP, Users agree to comply with this AUP and P&N's MTP Privacy Notice.**

Last Updated: October 26, 2021