COMPROMISO DE CONFIDENCIALIDAD

Nos dirigimos a Ud. en el marco del contrato de trabajo que mantiene vigente y de conformidad con la actual asignación para la prestación de servicios en instalaciones de la empresa TPS SA y/o cualquier de sus clientes, según las obligaciones del citado contrato a fin de dejar constancia de la incorporación al plexo de obligaciones del mismo de las normas sobre "Confidencialidad de la información y Seguridad de Acceso a los sistemas" que a continuación se enuncian y a las que, con relación a información, confidencialidad, seguridad informática y manejo de los recursos informáticos de propiedad de o suministrados por dicha empresa, deberá ajustar su conducta.

1. CONFIDENCIALIDAD DE LA INFORMACIÓN.

1.1 Todo empleado asume formalmente el deber de confidencialidad respecto de toda información y documentación a la que eventualmente pudiera acceder relativa a la organización, actividades, negocios y operaciones de cualquier tipo que llevara, estuviera analizando o tuviera previsto llevar a cabo, productos, información financiera y jurídica, etc. de su empleadora, de la empresa a la cual se encuentra actualmente asignado y/o de empresas vinculadas a cualquiera de ellas (en adelante denominadas en conjunto y o cualquiera de ellas en el presente capítulo "La Empresa"), se trate o no de aspectos previamente clasificados como reservados o confidenciales y cualquiera fuere el motivo y la vía utilizada para acceder a ellos.

Entre otros, Se consideran actos graves de incumplimiento de la obligación de confidencialidad a la divulgación, o el facilitamiento de la divulgación, por cualquier medio, de:

- Investigaciones y planes de nuevos productos;
- Objetivos comerciales y estrategias;
- Adquisiciones o ventas;
- Análisis internos en relación a reclamos de cualquier índole planteados por terceros o hacia terceros;
- Estados contables y financieros, así como toda la información y documentación que les sirviera de sustento;
- Secretos comerciales;
- Información no publicada vinculada con precios, líneas de productos, participación en mercados;
- Procedimientos y fórmulas;

- Cambios en la gerencia;

- Listados de empleados y cualquiera de sus datos;

- Información vinculada con salarios y beneficios;

- Información vinculada con seguros médicos de los empleados;

- Listados de clientes y proveedores, así como sus negocios, empleados, documentación, etc. y todo lo atiende a sus relaciones con la Empresa; y/o

- Cualquier otro aspecto inherente a emprendimientos y/o a actividades de cualquier tipo de la Empresa, incluyendo negociaciones y asociaciones con terceros, relaciones de todo tipo con autoridades gubernamentales o con otros terceros, etc.

1.2 Asimismo en relación a terceros deberá mantenerse la misma obligación de confidencialidad respecto de la información correspondiente a ellos a la que hubiera tenido acceso como consecuencia de su relación laboral con La Empresa.

1.3 El contenido de la presente obligación comprende, igualmente, la devolución inmediata de toda información que pudiera poseer en su poder el empleado al momento de la extinción de la relación laboral, cualquiera fuera su causa, así como la obligación de no divulgación de la misma, excepto que por disposiciones legales u órdenes judiciales (firmes o irrecurribles) se viera compelido a dar la información. En el primer caso se compromete a hacerlo previa información y consulta con La Empresa. En el caso de una orden judicial, se obliga a informar previamente a La Empresa.

1.4 Asimismo, la obligación de confidencialidad se extiende a toda la información a la que pudiera accederse, con o sin uso de passwords especiales, en la página de Intranet de la Empresa y de cualquiera de sus empresas directa o indirectamente vinculadas (tanto subsidiarias, como compañías controlantes o cuyo control -directo o indirecto- fuera de propiedad del mismo controlante de la Empresa).

1.5 La información de la Empresa sólo podrá ser utilizada para el cumplimiento de las obligaciones laborales del empleado frente a la Empresa y no podrá ser utilizada para beneficio personal del empleado (ni siquiera para formar parte de exposiciones académicas o de otro tipo salvo permiso expreso de un funcionario de la Empresa con autoridad suficiente a esos efectos) ni para beneficio de terceros de cualquier índole o naturaleza.

2. CONFIDENCIALIDAD Y SEGURIDAD INFORMÁTICA.

2.1 Habida cuenta que sólo las personas expresamente designadas por la empresa a la cual se encuentra actualmente asignado pueden ejecutar las operaciones o consultas de sistemas y/o archivos y/o bases de datos computarizados, para las cuales han sido expresamente autorizadas, por medio de su usuario habilitado y su clave de acceso o password, y toda vez que la misma es equivalente, como medio de identificación y a los efectos del acceso a los sistemas y a la información, a la firma personal, es responsabilidad mantener reserva y bajo su

exclusivo dominio el conocimiento y operación de su password, constituyendo falta de gravedad extrema: a) la divulgación de la misma; y/o b) su utilización hacia fines distintos o desviados respecto del específico cometido laboral asignado.

En tal sentido, el empleado declara conocer y aceptar la totalidad de las normas y procedimientos aplicables en materia de operación y seguridad informática aprobados por la empresa a la cual se encuentra actualmente asignado, y especialmente la prohibición absoluta e inderogable respecto del uso compartido de la password y su transferencia.

Queda especialmente comprendida dentro de la presente cláusula de confidencialidad y seguridad en el manejo de recursos informáticos, la obligación de proteger y de no revelar mecanismos de protección de las redes de voz y datos, sus componentes y sus passwords, resultando aplicable en lo pertinente, las definiciones contenidas en la presente norma.

2.2 En resguardo de dicha seguridad informática y en todo lo relativo, en relación a la definición y uso de su password todo empleado deberá respetar las siguientes pautas:

2.2.1 No armar la password con datos obvios fácilmente deducibles (por ej. nombres de hijos, cónyuge, fechas de nacimiento, etc.).

2.2.2 No prestar ni recibir passwords. Cuando sospechara que alguien la pudo descubrir, debe cambiarla mediante la vía prevista por el sistema.

2.2.3 No retirarse de la terminal dejando una sesión abierta. Siempre salir de la aplicación hasta la pantalla donde se ingresara la password.

2.3 En consecuencia, queda establecido que el conocimiento por parte de terceros de la password del empleado será en principio, objetivamente imputable a su incumplimiento del deber de confidencialidad, lo cual hará viable sin más la extinción del contrato de trabajo con justa causa, sin perjuicio aún de las acciones que pudieren corresponder por el resarcimiento de los daños y perjuicios que dicho incumplimiento le provocase a la empresa a la cual se encuentra actualmente asignado y/o a cualquier empresa vinculada.

2.4 De la misma manera, el intento por su parte de conocer o utilizar la password de un tercero, hará viable sin más la extinción del contrato de trabajo con justa causa, sin perjuicio aún de las acciones que pudieren corresponder por el resarcimiento de los daños y perjuicios que dicho incumplimiento le provocase a la empresa a la cual se encuentra actualmente asignado y/o a cualquier empresa vinculada.

2.5 Sin que ello implicare ninguna contradicción con los deberes de confidencialidad correspondiente a cada empleado, la empresa a la cual se encuentra actualmente asignado conservará sus facultades de control y verificación de todos los archivos, bases de información, electronics mails, correos de voz, conversaciones telefónicas y medios informáticos en general. En función de esto las personas designadas por su Dirección de Auditoria de la Empresa podrán en el marco de un ejercicio razonable de las facultades que le han sido asignadas

proceder a la apertura de dichas bases, mensajes de correo electrónico etc., con las limitaciones que la legislación aplicable pudiere imponer a esos efectos.

2.6 Sin perjuicio de la aplicación del régimen legal concerniente a la obligación de fidelidad a cargo del empleado, Las Partes convienen aceptar que el tratamiento y la regulación aquí acordada respecto del deber contractual de confidencialidad tendrán eficacia de ultraactividad respecto de la vigencia del contrato de trabajo, es decir que regirá aún con posterioridad a la extinción del mismo.

3. MANEJO DE LOS RECURSOS INFORMÁTICOS.

3.1 Todos los recursos tecnológicos puestos a disposición por la empresa a la cual se encuentra actualmente asignado para el desarrollo de las tareas, son propiedad de la misma y deben ser utilizados en orden al objetivo de su trabajo. Esto implica, en lo que hace a los recursos informáticos (computadores, pc, e-mail, redes, software, networks y cualquier información que circule a través de ellos, etc.), la no utilización de los mismos para objetivos ajenos al trabajo, sin la autorización expresa de la Gerencia de la empresa a la cual se encuentra actualmente asignado. Esto, en lo que hace al uso específico del mail o herramientas comunicacionales similares, implica también la no posibilidad de su uso para comunicaciones masivas ajenas al trabajo, como pueden ser "cadenas de saludos" u otras análogas.

3.2 Las siguientes situaciones están prohibidas:

- Participar en cualquier comunicación por vía electrónica que sea ofensiva, degradante, obscena, hostigante o que incluyera connotaciones discriminatorias sexuales, políticas, religiosas, raciales o étnicas o información vulgar.
- El uso de recursos tecnológicos para:
  - Diseminar en forma inapropiada materiales con patente o licencia registrada o información confidencial;
  - Violación de los términos de cualquier licencia de telecomunicaciones aplicable o cualquier ley de flujo de datos transborder (por ejemplo, leyes referidas a la recolección, protección, privacidad y confidencialidad de información); y/o
  - Desplegar actividades a través de cualquier modalidad que constituyera violación o el intento de violación de la legislación vigente.
- Intento de penetrar la seguridad de computadoras o redes de la empresa a la cual se encuentra actualmente asignado y/o a cualquier empresa vinculada u otro sistema, o el acceso no autorizado (o intento de acceso) a la computadora o a las cuentas o equipos de correo electrónico o de voz de cualquier otra persona, salvo que estas actividades fueran desarrolladas por las auditorias internas o externas siempre que contaren previamente con la autorización formal expresa de su Director de Auditoria de y/o sus empresas vinculadas.
- Visita de chat rooms o páginas de internet inapropiadas.

3.3 La falsificación electrónica no está permitida bajo ningún concepto. Cuando se reenvíen mensajes escritos por otros, deberán ser reenviados tal cual fueron recibidos y sin cambios (salvo autorización del autor), salvo que el empleado claramente identificare que el mensaje original fue modificado. El empleado no podrá enviar mensajes de correo electrónico utilizando la cuenta o casilla de otra persona, salvo que hubiera sido expresamente autorizado por el titular de la cuenta o casilla y sólo si el texto del mensaje indica el nombre del autor real del mensaje.

3.4 Dado que el uso de los recursos informáticos está regido por una estricta legislación en lo referente al manejo del software, está obviamente prohibido a todo el personal el uso de software no autorizado, o la copia de los mismos para usos personales o de terceros.

3.5 Es responsabilidad del empleado conocer las restricciones de uso o duplicación de software, requiriendo la información respectiva de modo de no violar los acuerdos de licencia, ni ejecutar actos que comprometan, directa o indirectamente, la responsabilidad de su empleadora.

3.6 Dada la repercusión que puede tener sobre la propia operatoria, como la de todo su sector o sociedad, es responsabilidad de cada empleado el tomar todas las precauciones en el manejo de los recursos informáticos garantizando el cuidado de la información mediante su archivo a través de la realización sistemática de backups y el cumplimiento de todas las medidas que hacen a la prevención de ingresos de virus en el sistema y de todo otro factor que pueda afectar la integridad del mismo.

El empleado declara haber leído y entendido el contenido de este documento y sus anexos, de corresponder, y que conoce los otros documentos a los que en él se hace referencia y que cumplirá con todas las regulaciones en él incluidas.

Por último, cumplo en informar a Ud. que presto expresa conformidad a fin de que mis datos personales y antecedentes laborales en v/poder sean incluidos en v/bases de datos, como así también al intercambio de dicha información con la empresa las empresas clientes de TPS SA. (en virtud de la relación comercial vigente) a fin de que ésta la incluya en las bases de datos correspondientes, sea a los fines de cumplimentar con obligaciones vigentes a cargo de esta empresa y/o de sus clientes a efectos de facilitar el control y gestión, como así también el intercambio de dicha información con empresas relacionadas, vinculadas, controlantes o controladas y/o terceras empresas.

COMPROMISO DE CONFIDENCIALIDAD

Nombre y Apellido del Empleado: _____
Empresa _____
CUIL _____
Fecha: __ de _____ de _____ Firma:_____
Nombre y Apellido del Apoderado de la Empresa: _____
Empresa _____
CUIL _____
Fecha: __ de _____ de _____ Firma:_____