นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของกรมการพัฒนาชุมชน

Website Security Policy of the Community Development Department

มาตรการและวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์

กรมการพัฒนาชุมชนได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูง ด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ 128 bits (128-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง ที่มีการทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของกรมการพัฒนาชุมชน ทำให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดยผู้ใช้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น https://www.rd.go.th

เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว กรมการพัฒนาชุมชนยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

- Firewall

เป็นระบบซอฟต์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิหรือผู้ที่กรมการพัฒนาชุมชนอนุมัติเท่านั้น จึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้

- Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอแล้ว กรมการพัฒนาชุมชนยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

- Cookies เป็นไฟล์คอมพิวเตอร์เล็ก ๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็นลงในเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไรก็ตามกรมการพัฒนาชุมชนตระหนักถึงความเป็นส่วนตัวของผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจำเป็นต้องใช้ Cookies กรมการพัฒนาชุมชนจะพิจารณาอย่างรอบคอบและตระหนักถึงความปลอดภัยและความเป็นส่วนตัวของผู้ขอรับบริการเป็นหลัก

- Auto Log off

ในการใช้บริการของกรมการพัฒนาชุมชนหลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย

แม้ว่ากรมการพัฒนาชุมชนจะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยปราศจากอำนาจตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังมิได้มีระบบรักษาความปลอดภัยใด ๆ ที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาดจากการถูกทำลายหรือถูกเข้าถึงโดยบุคคลที่

ปราศจากอำนาจได้
ดังนั้นท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ด้วยคือ
- ระมัดระวังในการ Download Program จาก Internet มาใช้งานควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login
เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์
-
ควรติดตั้งระบบตรวจสอบไวรัสไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรมตรวจสอบไวรัสในเครื่องของท่านมีความทันสมัยอยู่เสมอ
- ติดตั้งโปรแกรมประเภท Personal Firewall
เพื่อป้องกันเครื่องคอมพิวเตอร์จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker
- เก็บรักษา Username และ Password ของท่านไว้เป็นความลับ
ไม่ควรเปิดเผยหรือกระทำการที่อาจเปิดเผย Username และ Password ของท่านแก่บุคคลที่สาม

นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของกรมการพัฒนาชุมชน
Website Security Policy of the Community Development Department
จัดทำเมื่อวันที่ 15 กุมภาพันธ์ 2560

ประวัติความเป็นมาของโครงการ หนึ่งตำบล หนึ่งผลิตภัณฑ์

ในห้วงเวลาที่ประเทศชาติ กำลังเผชิญปัญหาวิกฤตทางเศรษฐกิจ และประชาชน ทุกระดับ ประสบปัญหาต่าง ๆปัญหาหนึ่งที่ประชาชนระดับรากหญ้า ซึ่งเป็นคนกลุ่มใหญ่ของประเทศถูกรุมเร้าคือปัญหาความยากจน รัฐบาลจึงได้ประกาศสงครามกับความยากจน
โดยได้แถลงนโยบายต่อรัฐสภาว่า
จะจัดให้มีโครงการหนึ่งตำบลหนึ่งผลิตภัณฑ์เพื่อให้แต่ละชุมชนได้ใช้ภูมิปัญญาท้องถิ่นมาใช้ในการพัฒนาสินค้าโดยรัฐพร้อมที่จะเข้าช่วยเหลือในด้านความรู้สมัยใหม่
และการบริหารจัดการเพื่อเชื่อมโยงสินค้าจากชุมชนสู่ตลาดทั้งในประเทศและต่างประเทศด้วยระบบร้านค้าเครือข่ายและอินเตอร์เน็ตเพื่อส่งเสริมและสนับสนุนกระบวนการพัฒนาท้องถิ่น
สร้างชุมชนให้เข้มแข็ง พึ่งตนเองได้ให้ประชาชนมีส่วนร่วมในการสร้างรายได้ด้วยการนำทรัพยากรภูมิปัญญาในท้องถิ่นมาพัฒนาเป็นผลิตภัณฑ์และบริการที่มีคุณภาพ มีจุดเด่นและมูลค่าเพิ่ม
เป็นที่ต้องการของตลาด ทั้งในและต่างประเทศและได้กำหนดระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการอำนวยการหนึ่งตำบล หนึ่งผลิต แห่งชาติ พ.ศ.2544 ประกาศ ณ วันที่ 7 กันยายน 2544 ขึ้น โดยกำหนดให้มีคณะกรรมการอำนวยการ หนึ่งตำบล หนึ่งผลิตภัณฑ์ แห่งชาติ
หรือเรียกโดยย่อว่า กอ.นตผ ซึ่งฯพณฯ นายกรัฐมนตรี ได้มอบหมายให้รองนายกรัฐมนตรี
(นายปองพล อดิเรกสาร) เป็นประธานกรรมการ และให้คณะกรรมการ กอ.นตผ
มีอำนาจหน้าที่ในการกำหนดนโยบาย ยุทธศาสตร์และแผนแม่บทการดำเนินงาน“หนึ่งตำบล หนึ่งผลิตภัณฑ์”
กำหนดมาตรฐานและหลักเกณฑ์การคัดเลือกและขึ้นบัญชีผลิตภัณฑ์ดีเด่นของตำบลรวมทั้งสนับสนุนให้การดำเนินงานเป็นไปตามนโยบาย ยุทธศาสตร์และแผนแม่บท อย่างมีประสิทธิภาพ

ปรัชญาของ หนึ่งตำบล หนึ่งผลิตภัณฑ์

“หนึ่งตำบล หนึ่งผลิตภัณฑ์” เป็นแนวทางประการหนึ่ง
ที่จะสร้างความเจริญแก่ชุมชนให้สามารถยกระดับฐานะความเป็นอยู่ของคนในชุมชนให้ดีขึ้น
โดยการผลิตหรือจัดการทรัพยากรที่มีอยู่ในท้องถิ่น ให้กลายเป็นสินค้าที่มีคุณภาพ
มีจุดเด่นเป็นเอกลักษณ์ของตนเองที่ สอดคล้องกับวัฒนธรรมในแต่ละท้องถิ่น
สามารถจำหน่ายในตลาดทั้งภายในและต่างประเทศ โดยมีหลักการ พื้นฐาน 3 ประการ คือ

1) ภูมิปัญญาท้องถิ่นสู่สากล (Local Yet Global)
2) พึ่งตนเองและคิดอย่างสร้างสรรค์ (Self-Reliance-Creativity)
3) การสร้างทรัพยากรมนุษย์ (Human Resource Development)
ผลิตภัณฑ์
ไม่ได้หมายถึงตัวสินค้าเพียงอย่างเดียวแต่เป็นกระบวนการทางความคิดรวมถึงการบริการ
การดูแลการอนุรักษ์ทรัพยากรธรรมชาติและสิ่งแวดล้อม การรักษา
ภูมิปัญญาไทย การท่องเที่ยว ศิลปวัฒนธรรม ประเพณี
การต่อยอดภูมิปัญญาท้องถิ่นการแลกเปลี่ยนเรียนรู้เพื่อให้กลายเป็นผลิตภัณฑ์ที่มีคุณภาพ
มีจุดเด่น จุดขายที่รู้จักกันแพร่หลายไปทั่วประเทศและทั่วโลก

วัตถุประสงค์ของหนึ่งตำบล หนึ่งผลิตภัณฑ์

จากนโยบายของรัฐบาล ที่แถลงต่อรัฐสภา
และตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการอำนวยการหนึ่งตำบล
หนึ่งผลิตภัณฑ์แห่งชาติ พ.ศ. 2544

การดำเนินงานตามโครงการหนึ่งตำบล หนึ่งผลิตภัณฑ์ มีวัตถุประสงค์เพื่อ

1) สร้างงาน สร้างรายได้ แก่ชุมชน
2) สร้างความเข้มแข็งแก่ชุมชน ให้สามารถคิดเอง ทำเอง ในการพัฒนาท้องถิ่น
3) ส่งเสริมภูมิปัญญาท้องถิ่น
4) ส่งเสริมการพัฒนาทรัพยากรมนุษย์

ส่งเสริมความคิดริเริ่มสร้างสรรค์ของชุมชน ในการพัฒนาผลิตภัณฑ์
โดยสอดคล้องกับวิถีชีวิตและวัฒนธรรมในท้องถิ่น

“The OTOP Website” (hereinafter “the Website”) specifically complies with the “The Regulation on Electronic Processing of Personal Data Protection”, for the protection of the Website’s data and your own, and implements the following Website Security Policy to state the Website’s security practices.

1. The Scope of the Policy

The following Website Security Policy is applicable to the collection, utilization, and protection of personal data when you are browsing the Website; however, it is not applicable to the other websites that are linked therefrom. When one follows links to other websites, the website security policies of that website apply.

2. The Control of Data Access

1) System data access and authorization requirements shall be implemented; written, electronic, or other means of notification shall be established to inform the staff and the users of the permissions and responsibilities of the site.
2) The authorization privileges for various data resources shall be immediately cancelled for staff who have resigned or have been terminated; this shall be regarded as the mandatory procedure for employment termination and resignation. For any adjustment or alteration of staff duty, authorization shall be adjusted within a certain period time according to the data access privileges of the new position.
3) A user registration management system shall be established to strengthen user password management. User passwords, in principle, shall not be used for a period longer than six months.
4) When system service vendors remotely log into the system for maintenance, security control measures shall be enhanced. A relevant roster shall be created for personnel with such responsibility.
5) An auditing system for data security shall be established to periodically or randomly execute data security audits.

3. The Website Security Procedures and Rules

Any unauthorized action to intentionally upload or modify any services provided by the office or other relevant information is strictly prohibited, and may be in violation of the law. In order to attain website security and to ensure that services can be uninterruptedly provided to all internal users, the Website delivers the following security protection measures:
1) At the points connecting to external networks, a firewall will be established to control data transfer and source access between the external and internal network and an identification process will be strictly enforced.
2) In order to identify unauthorized intentional intruders trying to upload or modify website information, an Internet intrusion detection system will be utilized to monitor the flow of network traffic.
3) Anti-virus software will be installed for periodic virus scans to ensure a safer browsing environment for the users.
4) A system backup system will be established to execute necessary data and software backup and stand-by operations in order to immediately resume regular operation in the event of disasters or storage media failure.
5) The simulation of hacker attacks shall be occasionally conducted to execute the system recovery drill in the event of security incidents and to provide a suitable security defense level.
6) Any classified and sensitive data or documents shall not be stored in the public data system; classified documents shall not be transmitted by electronic mail.
7) Electronic notifications about the security system and its maintenance will be automatically sent to all system and operation vendors. Patches will also be installed appropriately in accordance to the recommendations of such notices.
8) The Internet data transmission cannot guarantee 100 percent security; the Website will strive to protect the personal data of the Website and your own. In certain situations, a standard SSL security system will be utilized to ensure data transmission security. However, the data transmission process is influenced by your own Internet surfing environment. As we cannot guarantee the security of the data transmission from this Website, you must pay attention to and assume the risks involved in Internet data transmission. Please understand that any consequence resulting from this is beyond the Website’s control.

4. The security management of the firewall

1) A firewall will be established as a network relay server (such as Proxy Server) that provides the transport and control of Internet, services such as Telnet, FTP, and WWW.
2) The firewall will be the core of the entire network of this office. In case of unexpected events, a backup shall be prepared for all firewall host hardware and software.
3) The office's firewall system will routinely record the activities and incidents of the entire network. The data recorded—at minimum—shall include the date, time, originating IP, and communication protocol of the incident, for the purposes of routine management and future audit operations.
4) The log of the office's firewall will be examined and analyzed by firewall management personnel for any irregularities; such log shall be retained for at least one year.
5) In order to ensure the security of the firewall host computer, the office's firewall host computer shall only be logged into via system terminals; it shall not be logged into by any other method.
6) The security control setting of the office's firewall shall be reviewed frequently and adjusted as required to ensure that the goals of security control are attained.
7) The office's firewall system shall be backed up periodically. In addition, the backup shall be done on a stand-alone computer; any other method, including Internet backup, is not allowed.
8) The office's firewall system software will frequently update its version to be able to respond to a variety of network attacks.

5. The principles of data backup operation

1) The backup of significant data shall be maintained for at least three generations, in principle.
2) The backup data shall be protected by suitable physical and environmental measures; the safety standard shall match the safety standards of the major workplaces as much as possible. The computer security control measures of major workplaces shall be applied to backup operation workplaces as much as possible.
3) Periodic testing of backup data shall be conducted to ensure the usability of backup data.

6. Data recovery operation principles

1) When executing data recoveries, the consistency and completeness of the data shall be checked first.
2) When recovering website data, except in the event of unexpected major incidents resulting in difficulties for the computer facilities or network operation to recover, the data shall be restored to regular activities within 24 hours. The backup data shall be maintained and updated to the most recent data within two days to ensure that after the data has been recovered, programs and databases can all immediately resume normal operation.
3) Backup data shall be tested regularly to ensure its usability.
4) After the data recovery operation has been completed, relevant personnel shall continually monitor the system for three days to ensure its normal operation and the correctness of the newly added data.
7. Due to rapid technological advancement, the unfinished implementation of relevant regulations, and other future unforeseeable environmental changes, the data security policy is subject to be changed by the Website as required to ensure proper Internet security protection. After the Website has completed any amendments to the data security policy, we will immediately publish the new policy on the Website, and clearly highlight the amended sections for your reference.
8. For any questions or comments about the above terms and conditions, you are welcome to contact us through the details listed on the Website.