การลงทุนด้านเทคโนโลยีดิจิทัล ปีบัญชี 2563

ลำดับ	โครงการ	ระยะเวลาโครงการ	วัตถุประสงค์หรือประโยชน์ที่ได้รับ
1	**โครงการพัฒนาระบบรักษาความมั่นคงปลอดภัยรองรับ Cyber Resilience**	2563-2565	1. บริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารทางไซเบอร์ให้เป็นมาตรฐานสากลและเป็นไปตามข้อสังเกตของหน่วยงานกำกับดูแล 2. พัฒนาปรับปรุงระบบรักษาความ มั่นคงปลอดภัยด้านสารสนเทศให้รองรับ Cyber Resilience 3. จัดทำกระบวนการประเมินความเสี่ยงภัยคุกคามด้าน Cyber 4. ศึกษา วิเคราะห์ ทบทวนนโยบายและ วิธีปฏิบัติ ให้มีกรอบและทิศทางการดำเนินงานที่ชัดเจน 5. ส่งเสริมภาพลักษณ์ การมีระบบรักษาความมั่นคงปลอดภัย เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง และเพิ่มความเชื่อมั่นในการทำธุรกรรมให้กับลูกค้า 6. ลดความเสี่ยงและป้องกันภัยคุกคามที่มีโอกาสที่จะเกิดขึ้นกับระบบเทคโนโลยีสารนเทศขององค์กรทั้งภายในและภายนอก เพื่อให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ
2	**โครงการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**		เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับ พนักงานภายในองค์กร ลดความเสี่ยงและป้องกันภัยคุกคามที่มีโอกาสที่จะเกิดขึ้นกับระบบเทคโนโลยีสารนเทศขององค์กรทั้งภายในและ ภายนอก เพื่อให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ
3	**โครงการจัดจ้างที่ปรึกษาสำหรับการจัดทำกรอบธรรมาภิบาลด้านข้อมูลรวมจัดทำนโยบายด้านข้อมูล (Data Governance and Data policy) และให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)**		เพื่อให้มีการดำเนินการสำหรับจัดทำกรอบธรรมาภิบาลด้านข้อมูลรวมจัดทำนโยบายด้านข้อมูล (Data Governance and Data policy) และให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อให้ องค์กรดำเนินการจัดเก็บ ใช้ ข้อมูลต่างๆ สอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อช่วยลดความเสี่ยงที่อาจเกิดขึ้นต่อทรัพย์สินด้าน สารสนเทศต่างๆ ของธนาคาร

ลำดับ	โครงการ	ระยะเวลาโครงการ	วัตถุประสงค์หรือประโยชน์ที่ได้รับ
4	**โครงการจัดเช่าใช้บริการระบบเรียนรู้ Cyber Security (Sec Playground platform)**		เพื่อจัดหาระบบการเรียนรู้สำหรับพนักงานที่ปฏิบัติงานด้านความมั่นคงปลอดภัย ให้มีสถานที่ฝึกภาคปฏิบัติ ลดระยะเวลาการสอนงาน ได้ลงมือปฏิบัติจริงผ่านระบบการเรียนรู้
5	**โครงการจัดจ้างที่ปรึกษาสำหรับทบทวนนโยบายและวิธีปฏิบัติ สำคัญด้าน IT (ICT policy /IT outsource /Data protection) และประเมินความพร้อมด้านไซเบอร์ (Cyber Resilience) ตามกรอบ ธปท.**		เพื่อให้มีการกำหนดนโยบายและวิธีปฏิบัติสำหรับเป็นแนวทางปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศ ต่างๆ เช่น ICT policy **IT outsource** policy สอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศเพื่อช่วยลดความเสี่ยงที่อาจเกิดขึ้นต่อทรัพย์สินด้าน สารสนเทศต่างๆ ของธนาคาร
6	**จ้างบริการวิเคราะห์ภัยคุกคามอัจฉริยะ (Threat Intelligence)**		เพื่อให้องค์กรมีระบบการวิเคราะห์ภัยคุกคามอัจฉริยที่มี ประสิทธิภาพ เพื่อใช้เป็นข้อมูลส าหรับจัดการหากเกิดเหตุการณ์จาก การถูกโจมตีหรือภัยคุกคามทางไซเบอร
7	**โครงการพัฒนาระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัย**		จัดหาระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัย เพื่อรองรับการดำเนินธุรกิจของธนาคาร
8	**โครงการจ้างปรับปรุงการรักษาความมั่นคงปลอดภัยสารสนเทศให้ได้มาตรฐาน PCI-DSS**		เป็นการยกระดับบัตรเดบิตให้เป็นไปตามมาตรฐานความปลอดภัย สารสนเทศของ VISA และ PCI DSS เพื่อให้ลูกค้าผู้ถือบัตรเดบิตของ ธ.ก.ส. สามารถใช้เบิกเงินสดที่เครื่อง ATM ของธนาคารอื่นๆ ที่รองรับ VISA และ PCI DSS ได้ทั้งในประเทศและต่างประเทศ ท าให้ลูกค้า ได้รับความสะดวกในการใช้งาน
9	**โครงการจ้างตรวจประเมินตามมาตรฐาน PCI-DSS โดย QSA (PCI DSS Certification Service)**		เป็นการยกระดับบัตรเดบิตให้เป็นไปตามมาตรฐานความปลอดภัย สารสนเทศของ VISA และ PCI DSS เพื่อให้ลูกค้าผู้ถือบัตรเดบิตของ ธ.ก.ส. สามารถใช้เบิกเงินสดที่เครื่อง ATM ของธนาคารอื่นๆ ที่รองรับ VISA และ PCI DSS ได้ทั้งในประเทศและต่างประเทศ ท าให้ลูกค้า ได้รับความสะดวกในการใช้งาน

ลำดับ	โครงการ	ระยะเวลาโครงการ	วัตถุประสงค์หรือประโยชน์ที่ได้รับ
10	**โครงการจ้างปรับปรุงระบบรักษามั่นคงปลอดภัยด้าน ICT ให้รองรับ Cyber Resilience**		. บริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารทางไซเบอร์ให้เป็นมาตรฐานสากลและเป็นไปตามข้อสังเกตของหน่วยงานกำกับดูแล 2. พัฒนาปรับปรุงระบบรักษาความ มั่นคงปลอดภัยด้านสารสนเทศให้รองรับ Cyber Resilience 3. จัดทำกระบวนการประเมินความเสี่ยงภัยคุกคามด้าน Cyber 4. ศึกษา วิเคราะห์ ทบทวนนโยบายและ วิธีปฏิบัติ ให้มีกรอบและทิศทางการดำเนินงานที่ชัดเจน 5. ส่งเสริมภาพลักษณ์ การมีระบบรักษาความมั่นคงปลอดภัย เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง และเพิ่มความเชื่อมั่นในการทำธุรกรรมให้กับลูกค้า 6. ลดความเสี่ยงและป้องกันภัยคุกคามที่มีโอกาสที่จะเกิดขึ้นกับระบบเทคโนโลยีสารนเทศขององค์กรทั้งภายในและภายนอก เพื่อให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ